(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 351 102**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08105936 .2**
(96) Fecha de presentación : **01.03.2006**
(97) Número de publicación de la solicitud: **2066091**
(97) Fecha de publicación de la solicitud: **03.06.2009**

(54) Título: **Procedimiento para el autoaprovisionamiento de datos de abonado en el subsistema multimedia IP (IMS).**

(73) Titular/es:
NOKIA SIEMENS NETWORKS GmbH & Co. KG.
St. Martin Strasse 76
81541 München, DE

(45) Fecha de publicación de la mención BOPI:
31.01.2011

(72) Inventor/es: **Kieselmann, Gerhard;**
Schott, Markus y
Konecny, Martin

(45) Fecha de la publicación del folleto de la patente:
31.01.2011

(74) Agente: **Zuazo Araluze, Alexander**

DESCRIPCIÓN

Procedimiento para el autoaprovisionamiento de datos de abonado en el subsistema multimedia IP (IMS).

La invención se refiere a procedimientos y dispositivos para el registro de abonados en una red de telecomunicación móvil celular.

Los operadores móviles comienzan a ampliar sus ofertas de servicio con servicios proporcionados por medio del subsistema multimedia basado en IP (IMS) definido en las normas 3GPP de la versión 5 y superiores. Sin embargo, antes de que un abonado pueda usar cualquier servicio habilitado para IMS, al servidor de abonado residencial (HSS), que es la base de datos lógica central para los datos de abonado en las redes ver. >=5 de 3GPP, se le debe proporcionar información adicional relacionada con el abonado, por ejemplo la identidad de usuario privada IMS y la identidad pública IMS que se usan en el IMS para fines de identificación y direccionamiento.

Esta etapa de aprovisionamiento explícita aumenta los costes de administración de un operador e impide la introducción rápida de nuevos servicios. De manera ideal, un cliente de un operador existente interesado en usar un nuevo servicio simplemente obtendría un equipo de usuario (UE) capaz de proporcionar el nuevo servicio y empezaría a usarlo. Como máximo, se le pediría que realizara algunas etapas sencillas para configurar el UE.

Las soluciones conocidas para suministrar a un servidor de abonado residencial (HSS) información relacionada con el abonado como por ejemplo la identidad de usuario privada IMS y la identidad pública IMS que se usan en el IMS para fines de identificación y direccionamiento, son:

- El centro de atención al cliente (CCC) del operador crea los datos de suscripción IMS en el HSS antes de que el abonado pueda registrarse en el IMS y usar los servicios IMS.

Una desventaja de esta solución es que existe una etapa de administración adicional para el operador que aumenta los costes de operación y también es una barrera para la introducción rápida y fácil, dado que el usuario debe ponerse en contacto explícitamente con el operador.

- El propio usuario activa el aprovisionamiento proporcionando información específica a través del sitio web de un operador, por ejemplo. La información dada por el usuario se toma entonces como entrada para un procedimiento automatizado que crea los datos de abonado IMS y se proporciona al HSS.

Una desventaja de esta solución es que la información proporcionada por el usuario puede ser errónea, de forma intencionada o inadvertida y que por tanto la información debe verificarse y confirmarse cuidadosamente antes de aceptarla. [Los datos de abonado IMS también se requieren normalmente para cobrar por el servicio].

El documento WO 2004/019640 A1 da a conocer un procedimiento para identificar un terminal de usuario.

Es un objetivo de la invención permitir de manera eficaz suministrar a un servidor de abonado residencial HSS información relacionada con el abonado que pueda usarse en el IMS para fines de identificación y direccionamiento. El objetivo se soluciona mediante la invención definida en las reivindicaciones independientes.

La invención se refiere a un procedimiento que permite al HSS proveerse a sí mismo automáticamente y sobre la marcha de datos de abonado IMS cuando un usuario se registra en el IMS por primera vez. Para algunos servicios el HSS puede proveerse a sí mismo de todos los datos de abonado IMS requeridos para proporcionar el servicio; para otros servicios, el mecanismo sólo permite disminuir la cantidad de información que debe proporcionarse en una etapa de aprovisionamiento explícita adicional.

Suposiciones

La invención se basa en las siguientes suposiciones:

- La red de acceso (AN) que proporciona la conectividad de transporte IP subyacente para conectar el UE con el IMS puede autenticar el usuario. La AN es, por ejemplo, una red GPRS o WLAN. La suposición siempre se cumple en caso de una red de acceso GPRS o el dominio PS de una red UMTS.

- El UE se ha provisto previamente de todos los datos de configuración que le permiten registrarse en el IMS. Los detalles del aprovisionamiento de UE (mediante medios manuales o automatizados) no forma parte de esta invención. El conjunto de datos de configuración incluye, al menos, el nombre de dominio IMS, un nombre de dominio o dirección IP para acceder a la P-CSCF y una identidad de usuario pública IMS que se usa para el registro en el IMS. Si se realiza un procedimiento de autenticación entre el UE y el IMS, el UE también necesita conocer su identidad de usuario privada IMS (que se usa como “nombre de usuario” en el proceso de autenticación) y las claves (que es una “contraseña” en el caso más simple) requeridas para realizar la autenticación.

- El UE registra su identidad de usuario pública (y la relaciona con su dirección de contacto) a través del flujo de mensajes representado en la figura 1. El flujo descrito a continuación tiene aplicación para el caso de que al HSS

ya se le hayan proporcionado los datos de suscripción. No forma parte de la invención, pero define el marco para la invención.

La invención no requiere que el proceso de registro siga las especificaciones 3GPP en cada detalle. Sólo los detalles especificados en la descripción de la figura 1 son importantes. Esto significa que la invención funciona también y en particular con las denominadas implementaciones de "IMS inicial" que siguen las ideas y arquitectura de IMS generales, pero difieren en detalles.

N.º 1 *Autenticación y autorización mediante la AN (UE <-> AN)*

El UE se autentica mediante una función de autenticación y autorización (AA) de la AN a través de cualquier mecanismo y se autoriza para establecer conectividad IP con la P-CSCF. La autenticación se realiza basándose en un identificador de usuario AN, cuyos detalles dependen de la AN y el mecanismo de autenticación.

El UE también puede recibir parámetros de conectividad IP relevantes (por ejemplo su propia dirección IP) a través de este proceso, pero este detalle no es relevante en este contexto.

Ejemplo: si la AN es un GPRS, el UE solicita un contexto PDP del GGSN y también se le asigna una dirección IP en esta fase. El identificador de usuario AN es la IMSI.

N.º 2 SIP: *Registro (UE → P-CSCF)*

El UE envía un mensaje REGISTRO SIP a la P-CSCF con el fin de registrar su identidad de usuario pública IMS. La solicitud debe formularse conforme a la norma RFC 3261 de manera que la identidad de usuario pública usada para el registro esté en el encabezamiento Para de la solicitud. Si la implementación de IMS requiere un procedimiento de autenticación explícito, y dependiendo de los detalles de este procedimiento, el UE puede añadir un encabezamiento Autorización con un parámetro de nombre de usuario que contenga la identidad de usuario privada.

Ejemplo: si el IMS implementado se ajusta totalmente a las especificaciones 3GPP, el UE debe añadir un encabezamiento Autorización. Si es una implementación de "IMS inicial" que implemente el procedimiento de autenticación especificado en 3GPP TR 33.978, no se envía ningún encabezamiento Autorización.

N.º 3 SIP: *Registro (P-CSCF → I-CSCF)*

La P-CSCF envía la información recibida con la solicitud REGISTRO SIP al papel de I-CSCF. Que la información se transmita enviando realmente el mensaje SIP o por otros medios, es irrelevante. Por ejemplo, si el papel de I-CSCF se ubica conjuntamente con el papel de P-CSCF en el mismo servidor, la I-CSCF puede acceder a los datos a través de una estructura de datos interna.

N.º 4 *Solicitud de consulta de ubicación (I-CSCF → HSS)*

La I-CSCF consulta al HSS información con el fin de ubicar la S-CSCF. La solicitud contiene, en particular, la identidad de usuario pública recibida en la solicitud de registro. Puede contener la identidad de usuario privada, si se recibe con la solicitud de registro.

Que la solicitud y respuesta de consulta de ubicación se implementen según las especificaciones 3GPP TS 29.228 y TS 29.229 o no, es irrelevante para la invención.

N.º 5 *Respuesta a la consulta de ubicación (HSS → I-CSCF)*

El HSS comprueba si existe una entrada de abonado con esa identidad de usuario pública e identidad de usuario privada (si se envía con la solicitud). Si es así, envía una respuesta positiva que contiene o bien la dirección de la S-SCCF asignada a ese usuario o bien otra información que permite que la I-CSCF ubique una S-CSCF.

N.º 6 SIP: *Registro (I-CSCF → S-CSCF)*

La I-CSCF envía la información recibida con la solicitud REGISTRO SIP al papel de S-CSCF. Que la información se transmita enviando realmente el mensaje SIP o mediante otros medios, es irrelevante. Por ejemplo, si el papel de S-CSCF se ubica conjuntamente con el papel de I-CSCF en el mismo servidor, la I-CSCF puede acceder a los datos a través de una estructura de datos interna.

N.º 7a *Identificación (S-CSCF, HSS)*

En algunas implementaciones de IMS inicial, la AN puede evitar la falsificación de la dirección IP y la AA de AN puede proporcionar una relación de confianza entre el identificador de usuario AN (véase la etapa n.º 1) y la dirección IP del UE. La base de datos de abonados de HSS, por otro lado, puede tener el identificador de usuario AN almacenado junto con la entrada de suscripción IMS correspondiente. Esto permite realizar una correspondencia de la dirección IP del UE uno a uno con la entrada de suscripción en el HSS y, en particular, con las identidades de usuario privada y

pública de esta entrada de suscripción. El mensaje REGISTRO SIP recibido en la etapa n.º 6 contiene una identidad de usuario pública (y posiblemente una identidad de usuario privada) así como la verdadera dirección IP usada por el UE. Por tanto la S-CSCF puede identificar de manera segura al usuario por su dirección IP. Si el usuario usara una identidad de usuario pública falsificada en la solicitud REGISTRO SIP, la S-CSCF lo indicaría y rechazaría la solicitud.

Los detalles de la comunicación entre la AA de AN, el HSS y la S-CSCF que se necesitan para intercambiar la información requerida y llevar a cabo la correspondencia de datos son irrelevantes en este caso.

Esta etapa es opcional, si se ejecuta un procedimiento de autenticación real (etapa n.º 7b).

Ejemplo: Este principio se usa, por ejemplo, en la patente internacional WO 2004/019640 A1 y en la especificación 3GPP TS 33.978.

N.º 7b *Autenticación (UE <-> S-CSCF)*

En otras implementaciones de IMS, se realiza un procedimiento de autenticación entre el UE y la S-CSCF, por ejemplo el resumen HTTP (RFC2617) o el resumen AKA (RFC 3310). Esto requiere que el UE y la S-CSCF compartan las mismas claves. En este caso, no se requiere la etapa n.º 7a, de manera que las etapas n.º 7a y n.º 7b son opciones alternativas. Los detalles de la etapa que requieren otra ronda de mensajes SIP que van a intercambiarse, no son importantes para esta invención.

En algunas implementaciones, se realiza la etapa n.º 7b además de la etapa n.º 7a. Esto se realiza, por ejemplo, si el código de programa en el UE falla sin la secuencia de autenticación. En este caso, normalmente se usan claves ficticias que son idénticas para todos los UE.

Esto es similar al procedimiento de autenticación a menudo realizado por proveedores de servicios de Internet durante el establecimiento de la conexión PPP. Identifican al usuario por medio del número de teléfono y usan una contraseña ficticia publicada durante el establecimiento de la conexión PPP, solamente por motivos formales para garantizar que el código de los programas de acceso funcione correctamente.

N.º 8 *Asignación de servicio (S-CSCF <-> HSS)*

La S-CSCF solicita los perfiles de servicio y la lista de todas las identidades de usuario públicas asociadas con el registro (las denominadas identidades de usuario públicas registradas implícitamente).

N.º 9 SIP: *200 OK (S-CSCF → I-CSCF → P-CSCF → UE)*

La S-CSCF acusa el recibo del intento de registro. Las identidades de usuario públicas registradas implícitamente se transmiten al UE en el encabezamiento URI asociado a P.

Según una realización de la invención el HSS crea, sobre la marcha, una entrada de suscripción en su base de datos durante el primer intento de registro del usuario. En las redes IMS actuales, que sólo implementan los procedimientos tal como se esboza en la figura 1 y las explicaciones de esa figura, se rechazará tal solicitud.

Para una realización de la invención se describe adicionalmente bajo qué condiciones es posible un autoaprovisionamiento de HSS y según qué reglas se construye la suscripción. Esto se describe en la figura 2 con explicaciones adicionales que desarrollan la secuencia de actividades de la figura 1.

N.º 1b *Transferencia de identificador de usuario AN*

Después de que el usuario del UE se ha autenticado mediante la función AA de AN, se transfiere un único identificador de usuario AN al HSS. Este identificador también debe conocerlo el UE, por medio de una configuración previa, una consulta manual en la etapa n.º 2 a continuación, o cualquier otro medio.

[Además, si se ejecuta la etapa "7a Identificación", la dirección IP del UE debe transferirse además con el identificador de usuario AN, tal como ya se expuso en la descripción de la etapa n.º 7a en la sección de Suposiciones].

Esta etapa y la etapa n.º 4b son alternativas una de otra.

Ejemplo: en la red de acceso GPRS, se representa la AA de AN mediante el GGSN. El único identificador de usuario puede ser la IMSI, por ejemplo. La IMSI también es accesible para el UE, dado que se almacena en el módulo SIM o USIM. Dependiendo de los detalles de la implementación de red del operador, el MSISDN también puede servir como identificador. Esto es menos probable por varias razones, pero no se excluye por esta invención.

N.º 2 SIP: *Registro (UE → P-CSCF)*

La invención requiere que la identidad de usuario pública usada por el UE en este primer registro sea un URI de SIP sip: parte-usuario@dominio-operador, cuya parte-usuario se construye de una forma bien definida a partir del

identificador de usuario AN. El principio de construcción debe conocerse por el HSS. El UE o bien no envía ningún encabezamiento Autenticación con la solicitud, o bien envía un encabezamiento Autenticación con el parámetro nombre de usuario fijado a cualquier valor sintácticamente correcto.

Alternativamente, el UE puede usar cualquier cadena sintácticamente correcta como parte-usuario de la identidad de usuario pública, e insertar un encabezamiento Autenticación con el parámetro nombre de usuario fijado a una identidad de usuario privada que se construye de una forma bien definida a partir del identificador de usuario AN.

La implementación define la alternativa que se implementa, o si ambas alternativas existen conjuntamente.

Ejemplo: en combinación con una red de acceso GPRS y la IMSI como identificador de usuario AN, la identidad de usuario pública puede ser de la forma sip: valor-imsi@dominio-operador. En la 2ª alternativa, el parámetro nombre de usuario puede fijarse al valor IMSI y todos los UE pueden, por ejemplo, usar la misma identidad de usuario pública en esta etapa, por ejemplo: sip: ficticio@operador.net.

N.º 4 *Solicitud de consulta de ubicación (I-CSCF → HSS)*

El HSS recupera el identificador de usuario AN de o bien la identidad de usuario pública o bien la identidad de usuario privada, dependiendo de la alternativa elegida en la etapa n.º 2. El HSS busca en su base de datos una entrada de abonado que contenga el identificador de usuario AN. El identificador de usuario AN puede ser un elemento de datos separado en el registro de datos de abonado, o puede derivarse de otro elemento de datos del registro de datos de abonado, de la identidad de usuario privada, por ejemplo.

Si el HSS encuentra una entrada de abonado de este tipo, el procedimiento de registro se ejecuta adicionalmente tal como se describió en los comentarios de la figura 1.

Si el HSS no encuentra una entrada de abonado de este tipo, comprueba si un usuario con este identificador de usuario AN está actualmente autorizado por la AN para acceder al IMS. Si la función AA de AN ya ha notificado al HSS en la etapa n.º 1b, busca todas las notificaciones existentes para este identificador de usuario AN.

N.º 4b *Consulta de identificador de usuario AN (HSS <-> AA de AN)*

Alternativamente a la etapa n.º 1b, el HSS consulta a la AA de AN con el identificador de usuario AN recuperado en la etapa n.º 4 como entrada. Si un UE con este identificador de usuario AN está actualmente autorizado para acceder al IMS mediante la AN, la AA de AN responde a la consulta con una respuesta positiva. En caso de que se ejecute la etapa n.º 7a Identificación, la respuesta a la consulta también debe contener la dirección IP del UE.

Ejemplo: El HSS puede ejecutar una consulta de LDAP.

N.º 4c *Creación de entrada de abonado (HSS)*

Cuando el HSS ha verificado que el identificador de usuario AN recibido en la etapa n.º 4 pertenece a un UE que se ha autorizado por la AN, el HSS crea una nueva entrada de suscripción para el abonado asociado con el identificador de usuario AN. Se aplican las siguientes reglas:

• La identidad de usuario privada de la entrada de suscripción se crea a partir del identificador de usuario AN. La correspondencia debe ser biyectiva: esto significa que el algoritmo debe hacer corresponder el identificador de usuario AN con una única identidad de usuario privada y que debe haber una correspondencia inversa para recuperar el identificador de usuario AN de la identidad de usuario privada. En la mayoría de los casos, la correspondencia más simple será la correspondencia de identidad, es decir, la identidad de usuario privada es la misma que el identificador de usuario AN.

• La identidad de usuario pública de la entrada de suscripción o bien se fija a la identidad de usuario pública que el HSS ha recibido con la solicitud de consulta de ubicación, o bien se crea mediante el HSS a partir de cualquier otro dato y/o algoritmo que garantice un único valor. El procedimiento de creación debe garantizar que entradas de suscripción diferentes nunca tengan la misma identidad de usuario pública.

Además, es posible generar identidades de usuario públicas adicionales mediante cualquier algoritmo que garantice que las entradas generadas son únicas en toda la base de datos de suscripción.

• Si se realiza un procedimiento de autorización alternativamente a la identificación (véase la etapa n.º 8 en la figura 1), el HSS debe recuperar las claves correspondientes asociadas con el identificador de usuario AN de la AA de AN u otra base de datos en la red que tiene esta información. Si el procedimiento de autorización se ejecuta además del procedimiento de identificación, el HSS puede hacer lo mismo o simplemente crear la clave a partir de información configurada previamente. Esto es posible, dado que en este caso (autenticación además de identificación), la autenticación es una actividad meramente formal, en la que pueden usarse las mismas claves para todas las suscripciones.

• El perfil de servicio de la entrada de suscripción se crea a partir de una plantilla de perfil de servicio configurada previamente. Pueden estar disponibles varias plantillas de perfil de servicio y el HSS puede seleccionar la plantilla correcta para su uso mediante una regla de correspondencia basándose en el identificador de usuario AN. Si, por ejemplo, el identificador de usuario AN es la IMSI, el HSS puede almacenar diferentes perfiles de servicio para diferentes intervalos IMSI. También son posibles reglas de correspondencia más complejas.

[El perfil de servicio es una recopilación de datos relacionados con el usuario y el servicio. Contiene, por ejemplo, criterios de filtro que definen qué servidores de aplicación se invocan en solicitudes de comunicación SIP, e información de servicio adicional para estos servidores de aplicación. Véase la especificación 3GPP TS 29.228 para más detalles].

Ejemplo: si la AN es el GPRS, el GGSN actúa como AA de AN y si la IMSI se usa como identificador de usuario AN, el HSS puede fijar la identidad de usuario privada al IMSI. Con el fin de crear una identidad de usuario pública, el HSS puede consultar el MSISDN del usuario a partir del GGSN y fijar la identidad de usuario pública a sip: msisdn@dominio-operador. Supóngase que se realiza una autorización ficticia además de la etapa de identificación. Entonces el HSS rellenará la contraseña de resumen http (la "clave") con un valor configurado previamente. Evidentemente este valor también debe conocerlo cada UE.

Supóngase que la red solamente soporta un solo servicio PoC controlado por SIP (pulsar para hablar sobre celular). Entonces el perfil de servicio se crearía a partir de una sola plantilla de perfil de servicio que se escribió para este servicio.

N.º 7a *Identificación (S-CSCF, HSS)*

N.º 7b *Autenticación (UE <-> S-CSCF)*

N.º 8 *Asignación de servicio (S-CSCF <-> HSS)*

Estas etapas se realizan sin ninguna modificación requerida. En realidad, la S-SCCF ni siquiera sabe que el HSS construyó la entrada de abonado sobre la marcha.

N.º 9 SIP: *200 OK (S-CSCF → I-CSCF → P-CSCF → UE)*

Esta etapa tampoco se cambia. Los detalles de implementación y las políticas del operador pueden requerir bloquear la identidad de usuario pública que se usó durante el registro para su uso en la fase de comunicación. En este caso, un encabezamiento URI asociado a P debe contenerse en la respuesta 200 OK que contiene al menos una identidad de usuario pública que puede usarse para la comunicación. Esta identidad de usuario pública también se ha construido en la etapa n.º 4c.

Ejemplo: Supóngase que la identidad de usuario pública usada para el registro se construyó a partir de la IMSI que sirvió como identificador de usuario AN, por ejemplo como sip: valor-imsi@dominio-operador. La IMSI es un valor que no deben conocer las demás partes, para evitar ataques a la seguridad. Si el HSS conoce el valor MSISDN asociado con ese URI, puede crear otra identidad de usuario pública, por ejemplo sip: valor-msisdn@dominio-operador. Este valor se devolverá en el encabezamiento URI asociado a P, y la identidad de usuario pública derivada de IMSI usada para el registro se bloqueará para la comunicación.

Ejemplo

El siguiente ejemplo muestra una aplicación práctica de la invención.

La especificación 3GPP 3GPP TR 33.978 describe en detalle un procedimiento de registro simplificado para redes de acceso GPRS, en el que el procedimiento de autenticación se sustituye por un procedimiento de identificación. A veces se denomina este procedimiento "autenticación IMS inicial". Evidentemente, el procedimiento solamente funciona si el HSS ya dispone de todos los datos de suscripción relevantes. El procedimiento concuerda con el marco definido por la figura 1 y las explicaciones.

Este procedimiento puede mejorarse fácilmente con el autoaprovisionamiento de HSS según las reglas de esta invención. El mensaje fluye entre las entidades de red permaneciendo inalterado; la única diferencia es que el HSS crea un perfil de abonado sobre la marcha, si todavía no existe un perfil de este tipo. El UE y los papeles de CSCF no conocen este procedimiento de autoaprovisionamiento.

El procedimiento de registro convencional en caso de autenticación IMS inicial se representa en la figura 3. Se supone que el lector está familiarizado con este procedimiento. Las explicaciones de la figura 3 se concentran en los detalles relevantes para el autoaprovisionamiento de HSS. Cualquier actividad que sea una adición en comparación con el procedimiento convencional debido a las reglas de esta invención se marca con NUEVO.

N.º 1 *Activación de contexto PDP*

Esta etapa corresponde a la etapa n.º 1 de la figura 2, en la que la AN es un GPRS. El UE se identifica por su IMSI y se le asigna una dirección IP. Se configura el GGSN para evitar una falsificación de la dirección IP.

N.º 2 *Recuento de inicio RADIUS (GGSN <-> HSS)*

Con este mensaje, el GGSN notifica el MSISDN, la dirección IP y la IMSI del UE.

Si existe una entrada de abonado con este MSISDN, no se activa el autoaprovisionamiento y se ejecutan los procedimientos de autenticación comunes, tal como se explica en la especificación 3GPP TR 33.978.

NUEVO: si no existe ningún perfil de abonado con este MSISDN, el HSS almacena esta tupla de datos en una lista de datos Radius.

N.º 3 *Registro SIP (UE → P-CSCF)*

Se requiere por la especificación 3GPP TR 33.978 que el UE construya la identidad de usuario pública a partir de la IMSI almacenada en el SIM o USIM, según la siguiente regla:

Identidad de usuario pública: sip: [imsi]@ims.mnc[mnc].mcc [mcc].3gppnetwork.org

donde: [imsi] es el valor IMSI, [mnc] es el código de red móvil derivado de la IMSI y rellenado a la izquierda con dígitos "0" dando un número de 3 dígitos y [mcc] es el código de país para el servicio móvil.

Esto se ajusta a la regla de la invención de que la parte-usuario de la identidad de usuario pública se deriva a partir del identificador de usuario AN, que es la IMSI en este caso. No se envía ningún encabezamiento Autorización con la solicitud Registro.

Ejemplo para la identidad de usuario pública: sip: 234150999999999@ims.mnc015.mcc234.3gppnetwork.org

N.º 5 *Cx UAR / UAA (I-CSCF <-> HSS)*

Esta etapa corresponde a la secuencia de las etapas n.º 4, n.º 4c y n.º 5 en la figura 2.

Tal como se requiere por la especificación 3GPP TR 33.978, la I-CSCF envía una UAR (como solicitud de consulta de ubicación) que contiene la identidad de usuario pública y privada:

Identidad de usuario privada:

[imsi]@ims.mnc[mnc].mcc[mcc].3gppnetwork.org

Identidad de usuario pública: sip: [imsi]@ims.mnc[mnc].mcc[mcc].3gppnetwork.org

Nuevo:

A través del valor [imsi], el HSS puede identificar la tupla {IMSI, MSISDN, dirección IP} correspondiente recibida con el mensaje 2. Entonces el HSS crea un nuevo perfil de abonado para la identidad de usuario privada

[imsi]@ims.mnc[mnc].mcc[mcc].3gppnetwork.org

con la identidad de usuario pública fijada como

sip:x[msisdn]@[dominio-operador].

Ejemplo: sip:x49898901234567@mi-operador.com

Se deriva el perfil de servicio a partir de una plantilla de perfil de servicio configurada previamente. Supóngase que el HSS almacena varias plantillas de perfil para varios intervalos IMSI. Para determinar la plantilla correcta, el HSS comprueba la IMSI del nuevo abonado frente al intervalo IMSI configurado, y usa la plantilla apropiada.

N.º 7 *Cx MAR / MAA (S-CSCF <-> HSS)*

N.º 8 *Verificar la dirección IP (S-CSCF)*

Estas 2 etapas corresponden a la etapa n.º 7a Identificación de la figura 1 ó 2. La etapa n.º 7b Autenticación no existe en este caso.

N.º 9 *Cx SAR / SAA (S-CSCF <-> HSS)*

Esta etapa corresponde a la etapa n.º 8 de la figura 1 ó 2.

N.º *12. SIP 200 OK (P-CSCF → UE)*

El UE recupera, a partir del encabezamiento URI asociado a P, la identidad de usuario pública generada

sip: x[msisdn]@[dominio-operador].

Según la especificación 3GPP TR 33.978, el UE debe usar esta identidad de usuario pública para cualquier conversación SIP durante este periodo de registro; se bloquea la identidad de usuario pública derivada de la IMSI usada para el registro.

La realización de la invención comentada anteriormente puede tener las siguientes ventajas:

- El autoaprovisionamiento de HSS simplifica la introducción de servicios basados en IMS para el mercado de masas. El usuario puede comprar un terminal y empezar a usarlo.

- Se reducen los costes de administración para la introducción de servicios basados en IMS, dado que el centro de atención al cliente del operador no requiere crear entradas individuales de abonado en el HSS.

La invención permite el registro eficaz de un abonado para un subsistema multimedia de protocolo de Internet de una red de telecomunicación en la base de datos de abonados (HSS) del subsistema multimedia de protocolo de Internet. La invención se refiere a un procedimiento para crear una entrada de suscripción en la base de datos de abonados (HSS) del subsistema multimedia de protocolo de Internet de una red de telecomunicación, basándose en una identificación segura anterior del abonado mediante la red de acceso que concede acceso al subsistema multimedia de protocolo de Internet.

Referencias

3GPP TS 29.228 3GPP TS 29.228: “IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents”

3GPP TS 29.229 3GPP TS 29.229: “Cx and Dx interfaces based on the Diameter protocol; Protocol details”

3GPP TR 33.978 3GPP TR 33.978: “Security Aspects of Early IMS (Release 6)”

RFC 2617 IETF RFC 2617: “HTTP Authentication: Basic and Digest Access Authentication”

RFC 3261 IETF RFC 3261: “SIP: Session Initiation Protocol”

RFC 3310 IETF RFC 3310: “Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)”

Abreviaturas

3GPP	Proyecto de asociación para la 3ª generación
AA	Autenticación y autorización
AKA	Autenticación y acuerdo de clave
AN	Red de acceso
CCC	Centro de atención al cliente
GGSN	Nodo de soporte de pasarela GPRS
GPRS	Servicio general de radiocomunicación por paquetes
HSS	Servidor de abonado residencial
HTTP	Protocolo de transferencia de hipertexto

I-CSCF	Función de control de sesión de llamada interrogante
IMS	Subsistema multimedia basado en IP
IMSI	Identidad internacional de abonado móvil
IP	Protocolo de Internet
MAA	Respuesta de autenticación multimedia
MAR	Solicitud de autenticación multimedia
MSISDN	Número RDSI/PSTN internacional de estación móvil
P-CSCF	Función de control de sesión de llamada proxy
PDP	Protocolo de datos por paquetes
PoC	Pulsar para hablar sobre celular
PPP	Protocolo punto a punto
PS	Conmutado por paquetes
RADIUS	Marcación de autenticación remota en servicio de usuario
S-CSCF	Función control de sesión de llamada de servicio
SAA	Respuesta de asignación de servidor
SAR	Solicitud de asignación de servidor
SIM	Módulo de identidad de abonado
SIP	Protocolo de inicio de sesión
UAA	Respuesta de autorización de usuario
UAR	Solicitud de autorización de usuario
UE	Equipo de usuario
UMTS	Sistema universal de telecomunicaciones móviles
URI	Identificador de recursos uniforme
USIM	Módulo de identidad de abonado universal
WLAN	Red de área local inalámbrica

REIVINDICACIONES

1. Procedimiento para crear una entrada de suscripción en una base de datos de abonados de un subsistema multimedia de protocolo de Internet, que comprende

- conceder un acceso de abonado a través de una red de acceso a un subsistema multimedia de protocolo de Internet tras la identificación segura del abonado por medio de un único identificador de usuario de red de acceso,

- transmitir por el abonado el identificador de usuario de red de acceso en una solicitud de registro de un protocolo de inicio de sesión al subsistema multimedia de protocolo de Internet,

- transmitir mediante una función de control de sesión de llamada interrogante del subsistema multimedia de protocolo de Internet el identificador de usuario de red de acceso a una base de datos de abonados, y,

- crear y almacenar mediante la base de datos de abonados una entrada de suscripción con respecto al abonado si no existe ningún perfil de abonado para el abonado.

2. Procedimiento según la reivindicación 1, que comprende enviar mediante un dispositivo de acceso un mensaje con datos de identificación de abonado a la base de datos de abonados, cuando el abonado se registra por primera vez en el dispositivo de acceso para el subsistema multimedia de protocolo de Internet.

3. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que la transmisión del identificador de usuario de red de acceso en la solicitud de registro comprende transmitir solamente si no existe ninguna entrada de suscripción para este abonado en la base de datos de abonados.

4. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el identificador de usuario de red de acceso transmitido en la solicitud de registro no es el mismo identificador que el usado por la red de acceso para identificar al abonado, se usa una correspondencia para derivar el identificador de usuario de red de acceso usado por la red de acceso del identificador de usuario de red de acceso transferido en la solicitud de registro y se usa la correspondencia por la base de datos de abonados.

5. Procedimiento según cualquiera de las reivindicaciones anteriores, que comprende comprobar mediante la base de datos de abonados con la función de autenticación y autorización de la red de acceso, si el identificador de usuario de red de acceso recibido por medio de la función de control de sesión de llamada interrogante está actualmente autorizado para acceder al subsistema multimedia de protocolo de Internet, antes de crear y almacenar la entrada de suscripción para el abonado, si no existe ningún perfil de abonado.

6. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el identificador de usuario de red de acceso usado por la red de acceso comprende una identidad internacional de abonado móvil o un número RDSI internacional de estación móvil asociado con el abonado.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que la creación de la entrada de abonado comprende al menos uno de los siguientes:

i. crear una identidad de usuario privada de la entrada de abonado basándose en el identificador de usuario de red de acceso,

ii. establecer una identidad de usuario pública de la entrada de abonado como una identidad de usuario pública del usuario recibida en una solicitud de consulta de ubicación,

iii. crear un perfil de servicio de la entrada de abonado a partir de una plantilla de perfil de servicio configurada previamente.

8. Servidor de abonado residencial (HSS), que comprende

- medios para recibir una solicitud de consulta de ubicación para un usuario,

- medios para recuperar un identificador de usuario de red de acceso (AN) referido al usuario,

- medios para buscar si se halla una entrada de abonado asociada con el identificador de usuario de red de acceso (AN) en una base de datos de servidor de abonado residencial (HSS),

- medios para comprobar basándose en el identificador de usuario de red de acceso (AN), si no se halla ninguna entrada de abonado en la búsqueda, si el usuario asociado con el identificador de usuario de red de acceso (AN) está autorizado por la red de acceso para acceder a un subsistema multimedia de protocolo de Internet (IMS), y,

- medios para crear una entrada de abonado para el usuario si el resultado de la comprobación es que el usuario asociado con el identificador de usuario de red de acceso (AN) ha sido autorizado para acceder al subsistema multimedia de protocolo de Internet (IMS).

9. Servidor de abonado residencial (HSS) según la reivindicación 8, que comprende además medios para recibir, a partir de la red de acceso, el identificador de usuario de red de acceso (AN) referido al usuario, y en el que la comprobación comprende comprobar el identificador de usuario de red de acceso (AN) recibido.

10. Servidor de abonado residencial (HSS) según la reivindicación 8, en el que la comprobación comprende consultar la red de acceso (AN) con el identificador de usuario de red de acceso (AN) como entrada.

11. Servidor de abonado residencial (HSS) según la reivindicación 10, en el que la comprobación comprende recibir una respuesta a la consulta y el resultado de la comprobación se determina basándose en la respuesta.

12. Servidor de abonado residencial (HSS) según cualquiera de las reivindicaciones 8-11, en el que el identificador de usuario de red de acceso (AN) comprende uno de una identidad internacional de abonado móvil (IMSI) y un número RDSI internacional de estación móvil (MSISDN).

13. Servidor de abonado residencial (HSS) según cualquiera de las reivindicaciones 8-12, en el que la recuperación comprende recuperar el identificador de usuario de red de acceso (AN) de una identidad de usuario pública del usuario recibida en la solicitud de consulta de ubicación.

14. Servidor de abonado residencial (HSS) según cualquiera de las reivindicaciones 8-13, en el que la creación de la entrada de abonado comprende al menos uno de los siguientes:

iv. crear una identidad de usuario privada de la entrada de abonado basándose en el identificador de usuario de red de acceso (AN),

v. establecer una identidad de usuario pública de la entrada de abonado como una identidad de usuario pública del usuario recibida en la solicitud de consulta de ubicación,

vi. crear un perfil de servicio de la entrada de abonado a partir de una plantilla de perfil de servicio configurada previamente.

15. Servidor de abonado residencial (HSS) según cualquiera de las reivindicaciones 9-14, en el que la recepción desde la red de acceso comprende recibir una identidad internacional de abonado móvil (IMSI), un número RDSI internacional de estación móvil (MSISDN) y una dirección IP, y en el que el servidor de abonado residencial (HSS) se configura además para almacenar la identidad internacional de abonado móvil (IMSI), el número RDSI internacional de estación móvil (MSISDN) y la dirección IP, si no existe ninguna entrada de abonado asociada con el número RDSI internacional de estación móvil (MSISDN) en el servidor de abonado residencial (HSS).

FIG 1

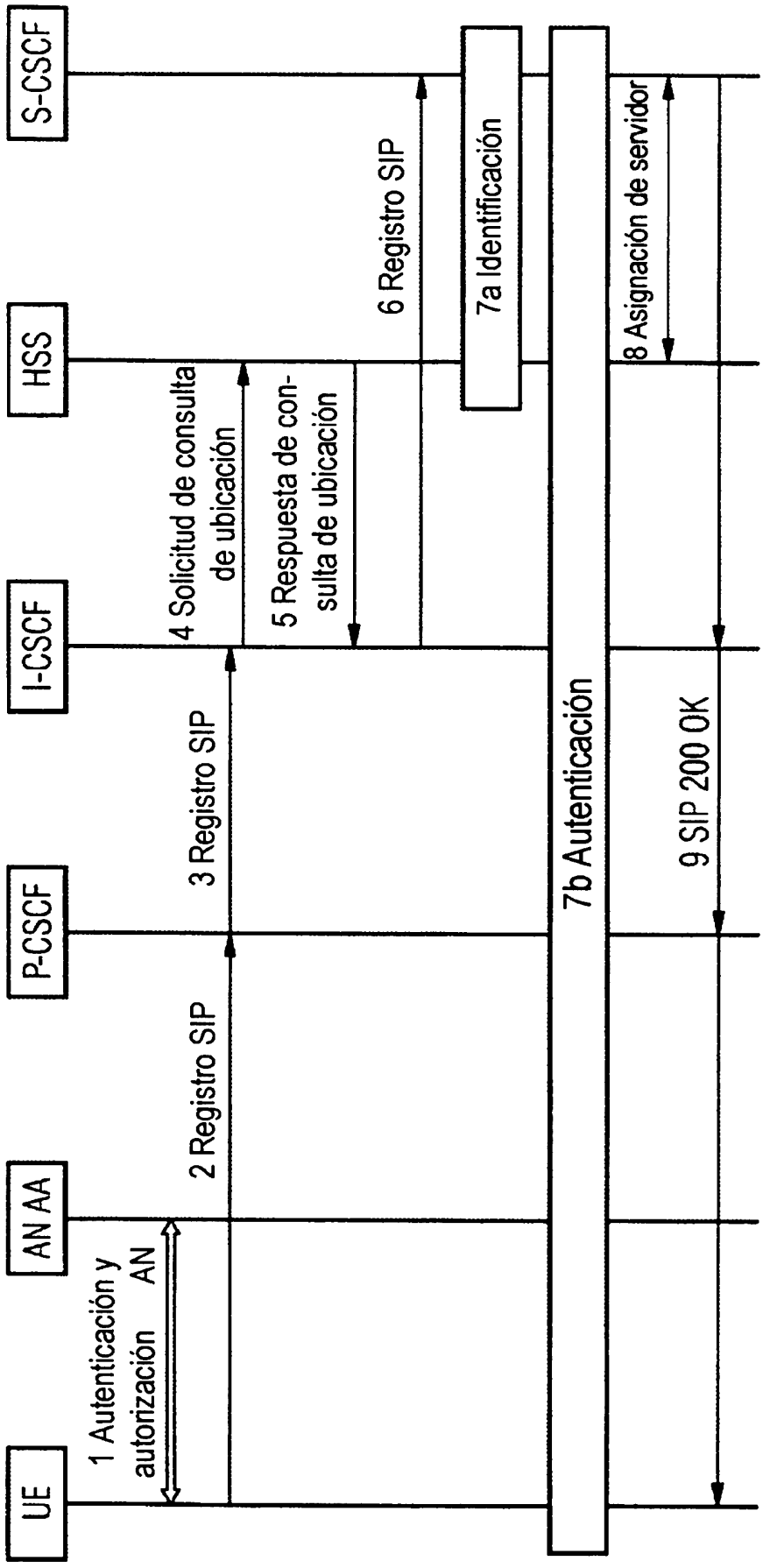

UE
AN AA
P-CSCF
I-CSCF
HSS
S-CSCF
1 Autenticación y autorización AN
2 Registro SIP
3 Registro SIP
4 Solicitud de consulta de ubicación
5 Respuesta de consulta de ubicación
6 Registro SIP
7a Identificación
7b Autenticación
8 Asignación de servidor
9 SIP 200 OK

FIG 2

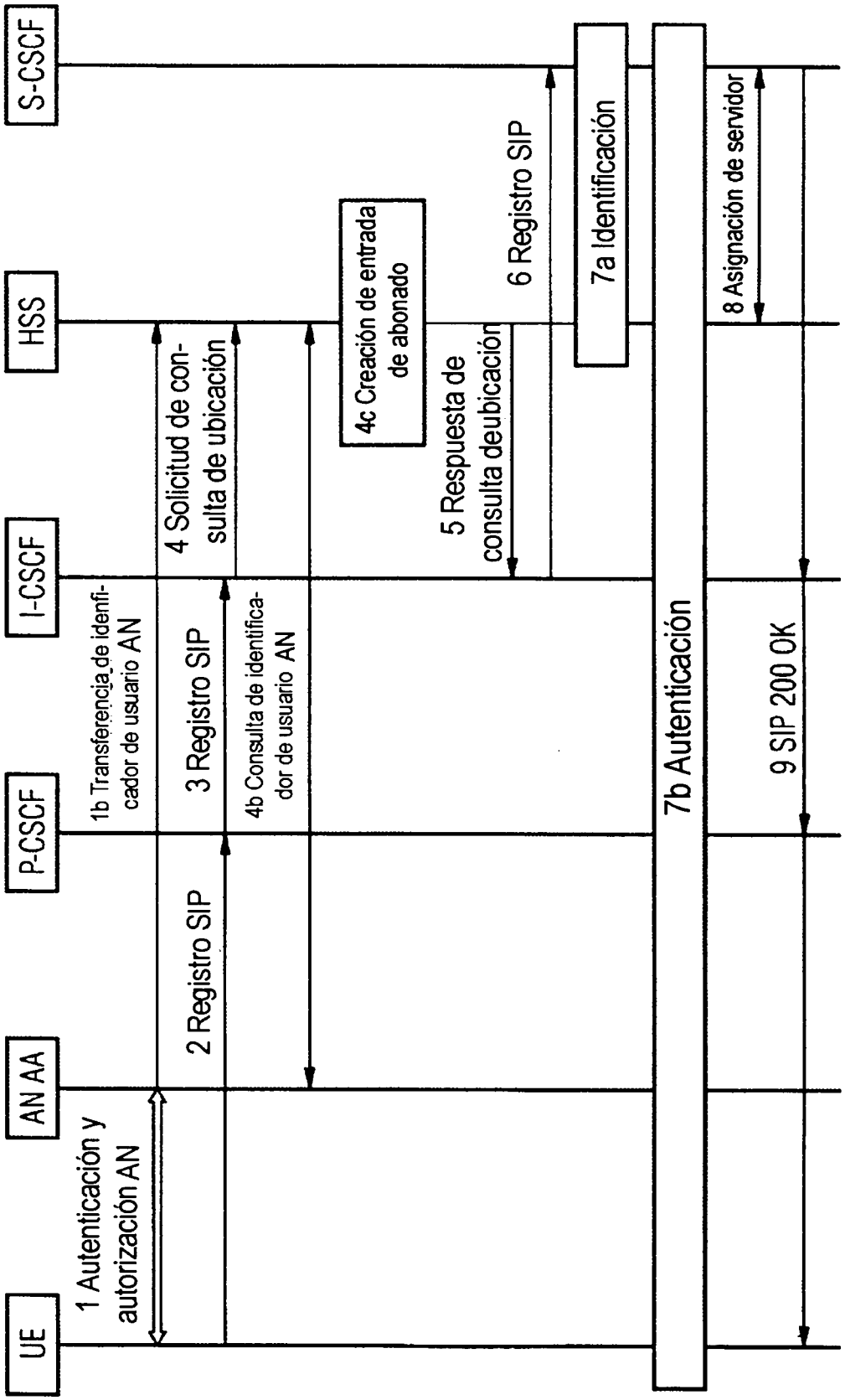
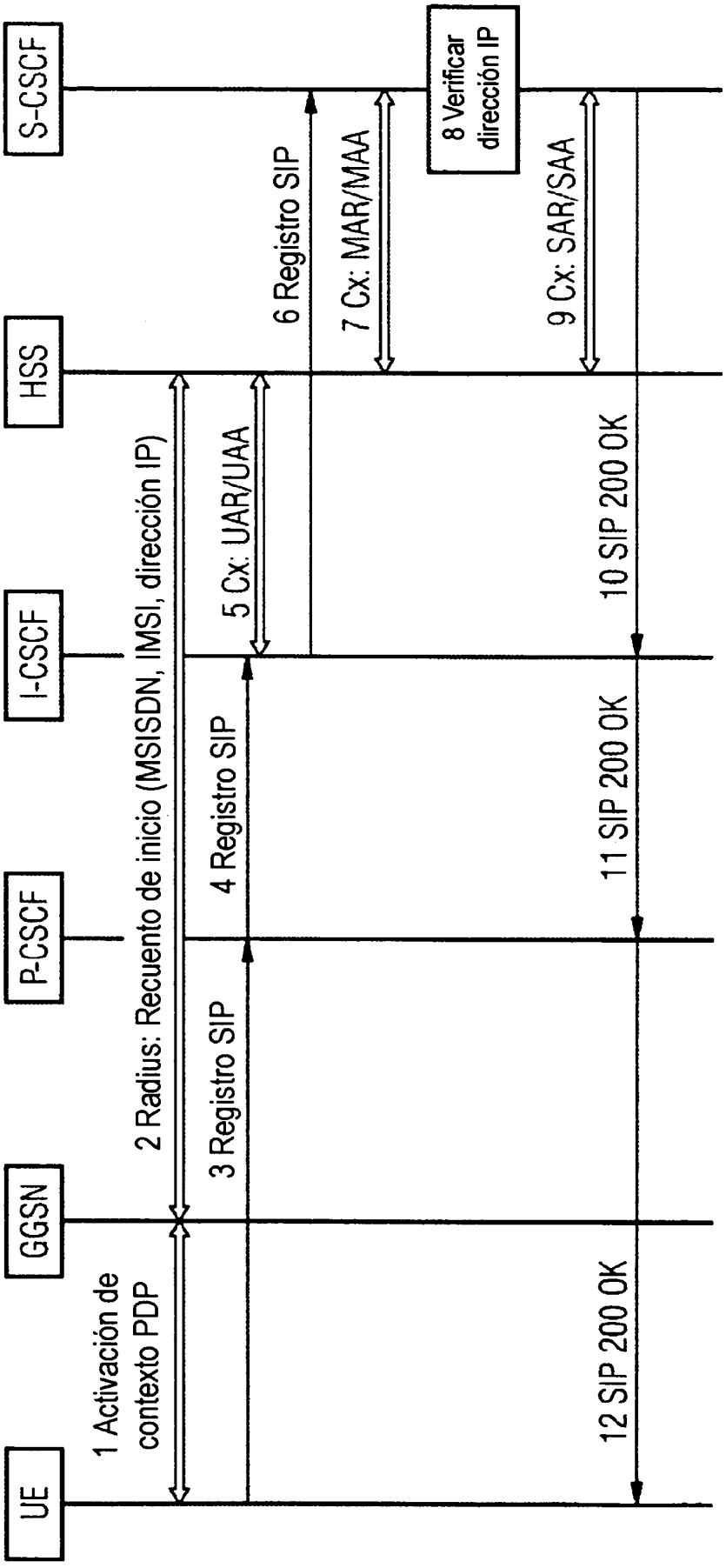

UE
AN AA
P-CSCF
I-CSCF
HSS
S-CSCF
1 Autenticación y autorización AN
1b Transferencia de identificador de usuario AN
2 Registro SIP
3 Registro SIP
4 Solicitud de consulta de ubicación
4b Consulta de identificador de usuario AN
4c Creación de entrada de abonado
5 Respuesta de consulta deubicación
6 Registro SIP
7a Identificación
7b Autenticación
8 Asignación de servidor
9 SIP 200 OK

FIG 3


UE
GGSN
P-CSCF
I-CSCF
HSS
S-CSCF
1 Activación de contexto PDP
2 Radius: Recuento de inicio (MSISDN, IMSI, dirección IP)
3 Registro SIP
4 Registro SIP
5 Cx: UAR/UAA
6 Registro SIP
7 Cx: MAR/MAA
8 Verificar dirección IP
9 Cx: SAR/SAA
10 SIP 200 OK
11 SIP 200 OK
12 SIP 200 OK