(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 362 924**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06791126 .3**
(96) Fecha de presentación : **26.09.2006**
(97) Número de publicación de la solicitud: **1953950**
(97) Fecha de publicación de la solicitud: **06.08.2008**

(54) Título: **Método, sistema y dispositivo para proteger una cuenta de servicio de redes.**

(30) Prioridad: **13.12.2005 CN 2005 1 0134640**

(45) Fecha de publicación de la mención BOPI:
15.07.2011

(45) Fecha de la publicación del folleto de la patente:
15.07.2011

(73) Titular/es: **HUAWEI TECHNOLOGIES Co., Ltd.**
Huawei Administration Building
Bantian, Longgang District, Shenzhen
Guangdong 518129, CN

(72) Inventor/es: **Shu, Qi y**
Zhong, Jieping

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

Método, sistema y dispositivo para proteger una cuenta de servicio de redes

Campo de la invención

La presente invención está relacionada con tecnologías de autentificación de servicios de redes y, particularmente, con métodos y sistemas para proteger una cuenta de servicio, dispositivos para almacenar un Perfil Personal de Comunicaciones (PCP) y servidores de aplicaciones.

Antecedentes de la invención

En la actualidad, la modalidad en cadena de la industria ha dado pasos gradualmente hacia una edad en que las aplicaciones son lo importante del pasado, cuando el acceso y la atención son lo importante. Los proveedores de contenidos han ocupado gradualmente un estado central en toda la cadena industrial. A lo largo de diversas aplicaciones proporcionadas por los proveedores de servicios, se han presentado también muchos problemas. Por ejemplo, fenómenos tales como el caballo Troyano y el robo de cuentas de servicio afectan seriamente el funcionamiento normal de los negocios en la red. Con el fin de restringir los fenómenos, los proveedores de negocios en la red proporcionan varios métodos. Sin embargo, los diversos métodos hacen incómodo el funcionamiento normal de los negocios en la red. Como revela la investigación, más del 65% de los usuarios tienen la experiencia de ser robados en la cuenta de servicio registrada en un servidor de aplicaciones. El problema de la seguridad de la cuenta de servicio se convierte en una pesadilla tanto para los operadores de negocios en la red como para los usuarios.

Actualmente, hay principalmente dos métodos para proteger la cuenta de servicio del usuario: un primer método de protección de teléfonos móviles y un segundo método de autentificación dinámica.

En el primer método, cuando el usuario entra en el servidor de aplicaciones, el servidor de aplicaciones genera una contraseña dinámica y envía la contraseña dinámica al teléfono móvil del usuario a través de una pasarela del Servicio de Mensajes Cortos (SMS) de un operador de red, de acuerdo con un número de teléfono móvil registrado por el usuario. Tras recibir la contraseña dinámica, el usuario entra en el servidor de aplicaciones utilizando la contraseña dinámica junto con una contraseña estática (Número de Identificación Personal, PIN). En el primer método, como nadie excepto el usuario puede obtener la contraseña dinámica, un usuario ilegal no puede entrar en el servidor de aplicaciones robando la contraseña del usuario.

El segundo método implica dos dispositivos para implementar la autentificación del usuario. Uno es un servidor de autentificación para autentificar la identidad del usuario. El otro es una tarjeta de contraseñas para generar una contraseña dinámica para el usuario. El servidor de autentificación y la tarjeta de contraseñas han sido instalados con el mismo software de generación de contraseñas y con un código de identificación que identifica unívocamente al usuario. Cuando el usuario obtiene la tarjeta de contraseñas, se carga el código de identificación en la tarjeta de contraseñas. Simultáneamente, se instala el código de identificación en una tabla de información del usuario de una base de datos del servidor de aplicaciones. El usuario tiene también un PIN recordado por uno mismo. Cuando el usuario entra en el servidor de aplicaciones e introduce el PIN, la tarjeta de contraseñas genera una contraseña dinámica que corresponde unívocamente a la tarjeta de contraseñas cada minuto, que es impredecible. La tarjeta de contraseñas envía la cuenta de servicio, el PIN y la contraseña dinámica al servidor de aplicaciones. El servidor de aplicaciones determina la legalidad y autenticidad del usuario de acuerdo con la contraseña dinámica. Como la contraseña dinámica se genera dinámicamente por la tarjeta de contraseñas, nadie excepto el usuario legal puede obtener la tarjeta de contraseñas y generar la contraseña dinámica correcta. Por tanto, la contraseña dinámica es inmune a ser observada y pinchada. Consecuentemente, el segundo método puede evitar el ataque de reenvío y es de alta seguridad y comodidad.

En los dos métodos para proteger la cuenta de servicio del usuario, el primer método tiene una limitación relativamente alta en la cuenta de servicio. Se requiere que la contraseña dinámica sea enviada cada vez al usuario por medio de un mensaje corto, y después el usuario introduce la contraseña recibida en el mensaje corto. Tiene un alto retardo de tiempo y desperdicia recursos de radio. En el segundo método, la protección está limitada a la cuenta de servicio de un solo proveedor de servicios. Más aún, cuando se utiliza el servicio, el usuario necesita comprar un hardware adicional, que frustra a la competencia de la aplicación.

Además, la solicitud de patente del Reino Unido (GB 2369543 A) divulga la presentación de información en un terminal desde una diversidad de fuentes, y más en particular un método para la presentación simultánea del contenido desde un cierto número de fuentes diferentes en un terminal de usuario. Además está relacionada con un método para establecer un enlace de comunicaciones entre el usuario y el servidor de aplicaciones. El método puede proporcionar preferiblemente el control de acceso a través de un motor de seguridad. El nivel de entrada para el usuario es un interfaz para entrar en el sistema, que puede ser respaldado por un certificado digital en el lado del cliente para un entorno de mayor seguridad. El proceso para la organización del contenido visual comprende los pasos siguientes: paso 510, el navegador de red utiliza un URL para abrir el enlace de comunicaciones desde el

cliente remoto al motor de páginas web; paso 520, al abrir el enlace de comunicaciones, el cliente es avisado para entrar en el sistema y el usuario entrega la información de entrada, que a su vez es enviada al servidor de aplicaciones; paso 525, el motor de seguridad comprueba la petición de entrada en el sistema respecto a la autenticidad; paso 530, en el caso de una entrada en el sistema con éxito, que genera una petición al servidor de la base de datos de un perfil de usuario apropiado en la base de datos de perfiles de usuario, y al recibir las particularidades requeridas, el usuario es autorizado para un nivel de acceso correcto de acuerdo con los privilegios del usuario en la base de datos de perfiles de usuario, y el interfaz de usuario es adaptado para el usuario de acuerdo con las preferencias del usuario en la base de datos de perfiles del usuario; paso 550, se descarga un sub-programa de desplazamiento por líneas al cliente; paso 560, se inicia el mecanismo de mensajería en línea.

Sumario de la invención

Los modos de realización de la presente invención proporcionan métodos y sistemas para proteger una cuenta de servicio, dispositivos para almacenar un Perfil Personal de Comunicaciones (PCP) y servidores de aplicaciones, para proteger convenientemente una cuenta de servicio de un usuario.

De acuerdo con un aspecto de la presente invención, un método para proteger una cuenta de servicio incluye:

autentificar la información de asociación cuando un usuario entra en un servidor de aplicaciones con una cuenta de servicio a través de un Equipo de Usuario (UE); si la autentificación tiene éxito, permitir al usuario entrar en el servidor de aplicaciones; en otro caso, rechazar al usuario para que no entre en el servidor de aplicaciones;

donde la información de asociación está configurada para la cuenta de servicio del usuario en un Perfil Personal de Comunicaciones (PCP) del usuario en un lado de la red.

De acuerdo con otro aspecto de la presente invención, un sistema para proteger una cuenta de servicio incluye:

un servidor de aplicaciones, adaptado para interactuar con un dispositivo de almacenamiento de PCP y un Equipo de Usuario UE, basándose en una petición de entrada en el sistema de un usuario, autentificar la información de asociación en un Perfil Personal de Comunicaciones (PCP) del usuario, y permitir que el usuario entre en el servidor de aplicaciones si la autentificación tiene éxito;

donde el dispositivo de almacenamiento de PCP está adaptado para almacenar el PCP del usuario; donde el PCP contiene información de asociación para la cuenta de servicio del usuario.

De acuerdo con otro aspecto de la presente invención, un dispositivo para almacenar un Perfil Personal de Comunicaciones (PCP) de un usuario incluye:

una base de datos de PCP, adaptada para almacenar un PCP de un usuario y la información de asociación para una cuenta de servicio del usuario;

una unidad de autentificación adaptada para recibir información de asociación, determinando si la base de datos de PCP comprende información de asociación consistente con la información de asociación recibida; y devolver un mensaje de éxito de la autentificación o un mensaje de fallo de la autentificación.

De acuerdo con otro aspecto de la presente invención, un servidor de aplicaciones para proteger una cuenta de servicio de un usuario incluye: una unidad de control de la entrada en el sistema y una unidad de comunicaciones; donde

la unidad de control de entrada en el sistema está adaptada para recibir una petición de entrada en el sistema a través de la unidad de comunicaciones; solicitar la información de asociación basada en la información de situación del PCP del usuario contenida en la petición de entrada en el sistema, determinar si la información de asociación recibida es consistente con la información de asociación almacenada en la unidad de control de entrada en el sistema, enviar un mensaje de éxito de la entrada en el sistema o un mensaje de fallo de la entrada en el sistema, a través de la unidad de comunicaciones.

En modos de realización de la presente invención, además de proteger la cuenta de servicio por medio de una contraseña estática, el usuario puede implementar una protección mejorada para la cuenta de servicio, sin recibir la contraseña dinámica a través de un mensaje corto, que reduce drásticamente el retardo de tiempo de entrada del usuario en el servidor de aplicaciones. Además, el usuario no necesita comprar adicionalmente la tarjeta de contraseñas. Por tanto, se mejora la competitividad del servidor de aplicaciones.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático que ilustra las relaciones de conexión de un servidor de PCP con un UE y un servidor de aplicaciones.

La figura 2 es un diagrama esquemático que ilustra la ubicación del servidor de PCP en la red del operador.

La figura 3 es un diagrama de flujo que ilustra un proceso de registro de una cuenta de servicio, de acuerdo con un modo de realización de la presente invención.

La figura 4 es un diagrama de flujo que ilustra un proceso de entrada en el sistema del usuario en el servidor de aplicaciones, de acuerdo con un modo de realización de la presente invención.

La figura 5 es un diagrama de flujo que ilustra un proceso de registro de una cuenta de servicio, de acuerdo con un modo de realización de la presente invención.

La figura 6 es un diagrama de flujo que ilustra un proceso de entrada en el sistema del usuario en el servidor de aplicaciones, de acuerdo con un modo de realización de la presente invención.

La figura 7 es un diagrama de flujo que ilustra un proceso de entrada en el sistema del usuario en el servidor de aplicaciones, de acuerdo con un modo de realización de la presente invención.

Modos de realización de la invención

La presente invención se describe con detalle de aquí en adelante, con referencia a los dibujos que se acompañan y a los modos de realización, para clarificar mejor las soluciones técnicas y ventajas de la presente invención.

A diferencia de los proveedores de servicios, los operadores de redes poseen recursos de red, mientras que los proveedores de servicios no los poseen. Los operadores de redes pueden proporcionar servicios básicos de acceso para los usuarios y una gestión de acceso uniforme, una autentificación de acceso y una autentificación del servicio, uniformes para los usuarios y los proveedores de servicios. Por tanto, la cuenta de servicio del usuario puede ser protegida combinando la autentificación del operador de la red con la cuenta de servicio del proveedor de servicios.

El operador de la red puede proporcionar un Perfil Personal de Comunicaciones (PCP) para el usuario, por medio de un número de acceso del usuario. El número de acceso puede ser un número de un terminal móvil proporcionado por un operador de móviles, un número de teléfono proporcionado por un operador de red fija o una cuenta de acceso proporcionada por un operador de banda ancha. El PCP es un conjunto mínimo completo establecido por el operador de red para el usuario y puede identificar unívocamente al usuario. Por ejemplo, el PCP puede incluir información de atributos de los recursos de servicio utilizados por el usuario en correspondencia con el PCP. Y la información de atributos de los recursos de servicio puede incluir atributos portadores de recursos de la red, un componente de la capacidad de servicio de capa superior, software de la plataforma y la aplicación, etc.

En modos de realización de la presente invención, la información de asociación para la cuenta de servicio del usuario se configura en el PCP del usuario proporcionado por el operador de la red. Cuando el usuario entra en un servidor de aplicaciones con la cuenta de servicio, la información de asociación en el PCP del usuario ha de ser autentificada. Si la autentificación tiene éxito, el usuario tiene permiso para entrar en el servidor de aplicaciones; en otro caso, el usuario es rechazado.

La autentificación de la cuenta de servicio puede ser realizada por el servidor de aplicaciones. Específicamente, el servidor de aplicaciones determina si la información de asociación configurada en el PCP del usuario es consistente con la información de asociación almacenada en el servidor de aplicaciones. Si la información de asociación en el PCP del usuario es consistente con la almacenada en el servidor de aplicaciones, la autentificación tiene éxito y la cuenta de servicio del usuario es legal; en otro caso, la autentificación falla y la cuenta de servicio es ilegal.

En modos de realización de la presente invención, la autentificación de la información de asociación puede ser realizada por un dispositivo relevante de PCP en la red del operador. En este caso, el servidor de aplicaciones envía la información de asociación almacenada en el servidor de aplicaciones al dispositivo relevante de PCP, el dispositivo relevante de PCP determina si la información de asociación recibida desde el servidor de aplicaciones es consistente con la almacenada en el dispositivo relevante de PCP, determinando con ello si la cuenta de servicio del usuario es legal.

En modos de realización de la presente invención, puede haber una pluralidad de cuentas de servicio correspondientes a un servicio. La información de asociación de la pluralidad de cuentas de servicio puede ser o no la misma. En otras palabras, la información de asociación se puede corresponder unívocamente con una cuenta de servicio, o corresponderse con una pluralidad de cuentas de servicio que pertenecen al mismo servicio y tienen un atributo común tal como un número de acceso.

La información de asociación puede ser un alias generado para la cuenta de servicio que registró el usuario. El alias se utiliza como identificador de asociación para asociar la cuenta de servicio y el PCP del usuario. De aquí en adelante, el identificador de la asociación se toma como ejemplo en los modos de realización de la presente invención.

En modos de realización de la presente invención, el PCP del usuario es almacenado en un dispositivo de almacenamiento de PCP que está situado en la red del operador. Específicamente, el dispositivo de almacenamiento de PCP puede ser un servidor de perfiles de Equipos de Usuario (UE), una base de datos de UE o un servidor de PCP, donde el servidor de PCP es denominado también unidad de gestión de PCP.

En la red del operador, la dirección del aparato de almacenamiento de PCP puede ser conocido de antemano por el servidor de aplicaciones, por ejemplo, cuando solamente hay un dispositivo de almacenamiento de PCP en la red del operador. La dirección del dispositivo de almacenamiento de PCP puede ser notificada también al servidor de aplicaciones cuando el usuario se registra o entra en el servidor de aplicaciones.

De aquí en adelante, el servidor de aplicaciones PCP se toma como ejemplo para ilustrar una estructura del sistema de acuerdo con un modo de realización de la presente invención. El servidor de PCP y las relaciones de conexión del servidor de PCP con los UE y el servidor de aplicaciones están ilustrados en la figura 1. En el sistema, el ordenador personal (PC) **101**, el teléfono móvil **102** y el Asistente Digital Personal (PDA) **103** son UE. El PC **101,** el teléfono móvil **102** y el PDA **103** tienen su respectivo PCP en el servidor **11** de PCP, y se conectan con el servidor **11** de PCP a través de la Pasarela de Acceso (AG) **10**.

Cada uno de los UE está configurado para enviar una petición de entrada en el sistema al servidor de aplicaciones, y está configurado también para recibir la información de ubicación del PCP desde el servidor **11** de PCP o recibir información de asociación desde el servidor **11** de PCP, y enviar la información de situación del PCP o la información de asociación al correspondiente servidor de aplicaciones a través de una petición de entrada en el sistema.

El servidor **11** de PCP está configurado para almacenar el PCP del usuario incluyendo la información de asociación del usuario; y está configurado también para enviar la información de asociación al servidor de aplicaciones como respuesta a una petición del servidor de aplicaciones, o para autentificar la información de asociación recibida desde el servidor de aplicaciones y devolver el resultado de la autentificación al servidor de aplicaciones.

El servidor de aplicaciones está configurado para interactuar con el servidor **11** de PCP, de acuerdo con la petición del usuario para entrar en el sistema, autentificar la información de asociación en el PCP del usuario y determinar el resultado de la entrada en el sistema de acuerdo con el resultado de la autentificación. Específicamente, el servidor de aplicaciones puede enviar una petición al servidor **11** de PCP de acuerdo con una petición del usuario para entrar en el sistema, solicitando la información de asociación del usuario y autentificar la información de asociación devuelta por el servidor **11** de PCP. El servidor de aplicaciones puede enviar también la información de asociación almacenada en el servidor de aplicaciones al servidor **11** de PCP, de acuerdo con la petición del usuario para entrar en el sistema. O bien, el servidor de aplicaciones autentifica la información de asociación contenida en la petición del usuario de entrada en el sistema, y devuelve un mensaje de éxito o fallo de la entrada en el sistema al UE, de acuerdo con el resultado de la autentificación.

El servidor **11** de PCP puede incluir una unidad **111** de generación de PCP, una unidad **112** de control de la gestión de PCP, una base de datos **113** de PCP, una unidad **114** de autentificación, una unidad **115** de interfaz con componentes del servicio y una unidad **116** de interfaz con la pasarela de acceso al servicio.

La unidad **111** de generación de PCP está configurada para gestionar el PCP del usuario, generar, actualizar y mantener el PCP de acuerdo con las órdenes de la unidad **112** de control de la gestión de PCP, y grabar el PCP generado, actualizado o mantenido en la base de datos **113** de PCP a través de la unidad **112** de control de la gestión de PCP.

El centro **112** de control de la gestión de PCP es un componente central del servidor **11** de PCP, está configurado para gestionar aplicaciones externas y componentes de interfaces de servicio, y además está configurado para gestionar la generación y almacenamiento del PCP.

La base de datos **113** de PCP está configurada para almacenar el PCP del usuario. La base de datos **113** de PCP puede incluir una pluralidad de dimensiones de datos de usuario. En modos de realización de la presente invención, los datos de usuario pueden ser la información de asociación. Las dimensiones pueden ser almacenadas en el formato siguiente en la base de datos **113** de PCP.

```
<?xml version="1.0" encoding="UTF-8"?>
 <PCPML>
  <PCPHdr>
    <PCPId>)0x56DFEA24F13</PCPId>            // Identificador de PCP
    <UserId>493005100592800</UserId>         //Identificador de usuario
```

...
</PCPHdr>
<PCPBody>
...<dimension name="Base Information" typeId="1"> // otra dimensión

</dimension>

<dimension name="PIM" typeId="2"> // dimensión de la cuenta de servicio

<item id="PIM001" name="WOW" type="ACC"> // elemento de cuenta de servicio 1

<Description> game name 1 </Description> // Descripción del elemento

<Meta> // descripción del tipo de cuenta

<Type xmlns="syncml:metinf"> application/Game.Account</Type>

<Format xmlns="syncml:metinf">b64</Format>

</Meta>

<ACL> read=www.wow.com-346&write= www.wow.com-346</ACL> // descripción de la Lista de Control de Acceso

<Data><!-- Base64-coded data--></Data>

// identificador de la asociación

< item >

<item id="PIM002" name="FWest" type="ACC"> //elemento de cuenta de servicio 2

<Description> game name 2 </Description> // descripción del elemento

<Meta> //description of the type of the account

<Type xmlns="syncml:metinf"> application/Game.Account</Type>

<Format xmlns="syncml:metinf">b64</Format>

</Meta>

<ACL>read=www.163.com-123&write= www.163.com-123</ACL>

// descripción de la Lista de Control de Acceso

```
<Data><!-- Base64-coded data--></Data>
                                                    // identificador de la asociación
<item>
...
</dimension>
<dimension name="Communication facilities" typeId="3">     // información de otras
...                                                          dimensiones
</dimension>
...
</PCPBody>
</PCPML>
```

El formato anterior de almacenamiento del PCP está basado en un Lenguaje de Marcación Extensible (XML). El fichero XML incluye una parte de Cabecera y una parte de Cuerpo.

La parte de Cabecera incluye información pública básica, tal como un identificador de PCP y un identificador de usuario, para identificar el usuario y el PCP del usuario.

La parte del cuerpo incluye valores de todos los parámetros relacionados con el PCP del usuario. Se utiliza una etiqueta <dimension> para que contenga todos los elementos de parámetros de la dimensión. Por ejemplo, <dimension name="PIM" typeId="2"> indica una dimensión de la cuenta de servicio; donde "name" indica el nombre de la dimensión; "typeId" es un identificador de la dimensión. Cada elemento de parámetro en la dimensión se identifica por un <ítem>. Cada dimensión puede incluir una pluralidad de elementos de parámetros.

El <ítem> puede incluir los siguientes parámetros: id, indica el nombre del elemento de parámetro y es un identificador exclusivo del elemento de parámetro en la dimensión; Name indica el nombre del elemento de parámetro; Type indica el tipo del elemento de parámetro. Específicamente, un <ítem>, es decir, un elemento de parámetro de la dimensión, se describe con los siguientes parámetros: <Description>, indica una descripción del elemento de parámetro; <Meta> indica el tipo (Type) y el formato (Format) del elemento de parámetro; <ACL> indica una Lista de Control de Acceso del elemento de parámetro; y <Data> indica un valor del elemento de parámetro. El <Meta> incluye dos elementos: <Type> indica el tipo del elemento de parámetro, y <Format> indica el formato del elemento de parámetro. En un fichero de descripción, cada elemento de parámetro puede estar provisto de un tipo predeterminado. Por ejemplo, si no hay un <Meta> en los datos de PCP, el valor del elemento de parámetro es el tipo predeterminado. Como se describe a continuación, una cuenta de servicio es un Item.

```
<item id="PIM001" name="WOW" type="ACC">     // elemento de cuenta 1 de servicio
<Description> game name 1 </Description>     // descripción del elemento
<Meta>                    // description of the type of the account
<Type xmlns="syncml:metinf"> application/Game.Account</Type>
<Format xmlns="syncml:metinf">b64</Format>
</Meta>
<ACL>        read=www.wow.com-346&write=        www.wow.com-
346</ACL>                                  // descripción de la Lista de Control de Acceso
<Data><!-- Base64-coded data--></Data>     // identificador de asociación
<item>
```

En la descripción anterior, “read=www.wow.com-346&write=www.wow.com-346” es la descripción del servidor de aplicaciones, que adopta un formato de la dirección del servidor de aplicaciones. Esto indica que solamente la petición desde esta dirección es del servidor de aplicaciones correspondiente al Item, y las funciones de lectura y escritura pueden ser realizadas para el siguiente identificador de asociación <!--Base64-coded data-->.

La unidad **114** de autentificación autentifica los recursos de la red y los recursos de servicios utilizados por el usuario, basándose en el PCP del usuario; envía la información de la ubicación del PCP del usuario al UE, recibe una petición desde el servidor de aplicaciones solicitando el identificador de asociación, obtiene el identificador de asociación desde la base de datos **113** de PCP y envía el identificador de asociación al servidor de aplicaciones; o envía el identificador de asociación del PCP del usuario al UE; o recibe el identificador de asociación desde el servidor de aplicaciones y autentifica si la base de datos **113** de PCP incluye un correspondiente identificador de asociación y devuelve el resultado de la autentificación al servidor de aplicaciones.

La unidad **115** de interfaz con componentes del servicio se utiliza para conectar comunicativamente la unidad **112** de control de la gestión de PCP y la unidad **114** de autentificación con los UE por medio del AG **10**, y para conectar comunicativamente la unidad **112** de control de la gestión de PCP y la unidad **114** de autentificación con otros elementos de la red del operador.

La unidad **116** de interfaz con la pasarela de acceso al servicio abierto se utiliza para conectar comunicativamente la unidad **112** de control de la gestión de PCP y la unidad **114** de autentificación con el servidor de aplicaciones, a través de la pasarela **12** de servicio abierto.

Los servidores **121, 122, 123**,… de aplicaciones están conectados comunicativamente con la unidad **112** de control de la gestión de PCP, respectivamente, a través de la pasarela **12** de servicio abierto.

Cada uno de los servidores de aplicaciones incluye una unidad **1201** de comunicaciones y una unidad **1202** de control de entrada en el sistema.

La unidad **1201** de comunicaciones se utiliza para conectar comunicativamente la unidad **1202** de control de entrada en el sistema con los UE y el servidor **11** de PCP.

La unidad **1202** de control de entrada en el sistema se utiliza para recibir la solicitud de entrada en el sistema desde el UE a través de la unidad **1201** de comunicaciones, y para autentificar el identificador de asociación contenido en la petición de entrada en el sistema; determinar el resultado de la entrada en el sistema basándose en el resultado de la autentificación, y enviar el resultado de la entrada en el sistema al UE, a través de la unidad **1201** de comunicaciones; o enviar el correspondiente identificador de asociación almacenado en la unidad **1202** de control de entrada en el sistema al servidor **11** de PCP, de acuerdo con la información de ubicación del PCP contenida en la petición de entrada en el sistema; recibir el resultado de la autentificación devuelto por el servidor **11** de PCP; determinar el resultado de la entrada en el sistema basándose en el resultado de la autentificación y enviar el resultado de la entrada en el sistema al UE a través de la unidad **1201** de comunicaciones; o solicitar al servidor **11** de PCP el correspondiente identificador de asociación basándose en la información de ubicación del PCP contenida en la petición de entrada en el sistema; determinar si el identificador de asociación es consistente con el identificador de asociación almacenado en la unidad **1202** de control de entrada en el sistema; determinar el resultado de la entrada en el sistema basándose en el resultado de la autentificación, y enviar el resultado de la entrada en el sistema al UE, a través de la unidad **1201** de comunicaciones.

La figura 1 es un diagrama esquemático que ilustra una estructura de un servidor de PCP y las relaciones de conexión del servidor de PCP con el UE y el servidor de aplicaciones. El servidor de PCP en la red del operador puede estar situado en una capa que contiene la capacidad común, como se ilustra en la figura 2. Otros componentes de la arquitectura de la red, excepto el servidor de PCP en la capa que contiene la capacidad común, pueden ser implementados de acuerdo con la técnica relacionada y no se describirán con detalle en este documento.

El método de la presente invención se describe de aquí en adelante en detalle, con referencia a los modos de realización que se acompañan.

Un primer modo de realización de la presente invención incluye un proceso de registro y un proceso de entrada en el sistema, ilustrados respectivamente en la figura 3 y en la figura 4.

El proceso de registro está ilustrado en la figura 3 e incluye específicamente:

Bloque **301**: Un usuario accede a la red del operador a través de un UE. En este bloque, el usuario puede acceder a la red del operador, a través de un terminal inalámbrico o fijo.

Bloque **302**: Un servidor de PCP en la red del operador obtiene el PCP del usuario, de acuerdo con un identificador de acceso del usuario.

En este bloque, el servidor de PCP puede buscar, de acuerdo con el identificador de acceso del usuario, una base de datos de PCP para el PCP del usuario. Si el usuario accede a la red por primera vez y no hay PCP para el usuario, se puede incluir también un bloque de inicialización. En el bloque de inicialización, el servidor de PCP genera un PCP para el usuario.

Bloque **303:** El servidor de PCP realiza la autentificación de la red y la autentificación del servicio para el usuario.

La autentificación de la red y la autentificación del servicio en este bloque significan autentificar la información en el PCP del usuario, puede incluir la autentificación del atributo de capacidad de la red y la capacidad del servicio básico en el PCP. La autentificación del atributo de la capacidad de la red incluye: las autentificaciones de la capa de control de la red, basándose en la información relevante del PCP del usuario, la capacidad del portador del usuario tal como el ancho de banda de acceso y la Calidad del Servicio. La autentificación de la capacidad del servicio básico se refiere a la autentificación de la capacidad de servicio del usuario, tal como el SMS, el servicio de localización, etc., pero no la autentificación de un servicio específico. Si la autentificación tiene éxito, indica que el usuario puede utilizar la red normalmente. Las implementaciones de la autentificación de la red y la autentificación del servicio son similares a la técnica relacionada. La diferencia es que, en los modos de realización de la presente invención, es el servidor de PCP el que realiza la autentificación y el PCP del usuario proporciona datos para la autentificación de la red y la autentificación del servicio.

Bloque **304**: El servidor de PCP envía información de localización del PCP al UE. La información de localización del PCP puede ser la dirección del servidor de PCP, tal como un Localizador de Recursos Uniformes (URL) del servidor de PCP. El servidor de PCP puede enviar también un modo de interacción, un certificado u otra información al UE para la autentificación entre el servidor de PCP y el UE.

Bloque **305:** El usuario envía una petición de registro al servidor de aplicaciones cuando se registra una cuenta de servicio en el servidor de aplicaciones. La información de localización del PCP puede estar contenida en la petición de entrada en el sistema.

Bloque **306**: Tras recibir la petición de registro, el servidor de aplicaciones envía un mensaje al usuario para indagar si debe asociar la cuenta de servicio del usuario con el PCP del usuario.

Bloque **307**: Tras recibir el mensaje, si el usuario determina que hay que asociar la cuenta de servicio con el PCP del usuario, continuar en el Bloque **308**; en otro caso, continuar en el Bloque **309**.

Bloque **308**: El usuario devuelve un acuse al servidor de aplicaciones. La información de localización del PCP puede ser enviada también al servidor de aplicaciones en este bloque, en lugar del bloque **305**. Si la información de localización del PCP es enviada al servidor de aplicaciones en este bloque, continuar en el bloque **310**; en otro caso, continuar en el bloque **309.**

Bloque **309**: El usuario devuelve un mensaje de rechazo de la asociación al servidor de aplicaciones.

Bloque **310**: El servidor de aplicaciones genera un identificador de asociación para el usuario, almacena el identificador de asociación en el servidor de aplicaciones, y envía el identificador de asociación al servidor de PCP de acuerdo con la información de localización del PCP, por medio de un mensaje de solicitud de asociación. El mensaje de solicitud de asociación incluye además un identificador de usuario u otra información de la dimensión.

Bloque **311**: Tras recibir el mensaje de solicitud de asociación, el servidor de PCP envía un mensaje de aviso al UE para avisar al usuario de que hay un servidor de aplicaciones solicitando asociar la cuenta de servicio del usuario con el PCP del usuario. El mensaje de aviso incluye información del servidor de aplicaciones.

Bloque **312**: Tras recibir la petición de aviso, si el usuario determina que ha de asociar la cuenta de servicio con el PCP, se continúa en el bloque **313**; en otro caso, continuar en el Bloque **314**.

Bloque **313**: El usuario devuelve un acuse al servidor de PCP y continúa en el bloque **315**.

Bloque **314**: El usuario devuelve un mensaje de rechazo al servidor de PCP. El servidor de PCP puede devolver también un mensaje de rechazo al servidor de aplicaciones y el servidor de aplicaciones devuelve un mensaje de fallo del registro al UE.

Bloque **315**: Tras recibir el acuse desde el UE, el servidor de PCP añade el identificador de asociación recibido desde el servidor de aplicaciones del PCP del usuario y devuelve un mensaje de éxito de actualización al servidor de aplicaciones. En este bloque, el servidor de PCP puede añadir también otra información relacionada contenida en el mensaje de petición de asociación al correspondiente elemento del PCP del usuario.

Bloque **316**: Tras recibir el mensaje de éxito de la actualización, el servidor de aplicaciones devuelve un mensaje de éxito del registro de la cuenta de servicio al usuario.

El proceso de entrada en el sistema del usuario correspondiente al proceso de registro, está ilustrado en la figura 4. Los bloques **401** a **404** son similares a los bloques **301** a **304** de la figura 3, y el Bloque **405** se efectúa tras el Bloque **404**.

Debido a que el servidor de PCP ha enviado la información de localización del PCP del usuario al UE durante el proceso de registro, el UE puede almacenar la información de localización del PCP. Por tanto, en el proceso de entrada en el sistema, el servidor de PCP no puede enviar la información de localización del PCP al UE en el Bloque **404**. En lugar de eso, el servidor de PCP envía la información de autentificación de la red y la información de autentificación del servicio al UE.

Bloque **405:** después de que el usuario haya introducido la cuenta y la contraseña de entrada en el sistema, el UE envía una petición de entrada en el sistema al servidor de aplicaciones que contiene la cuenta de entrada en el sistema, la contraseña y la información de localización del PCP almacenada en el UE.

Bloque **406**: El servidor de aplicaciones autentifica la legalidad de la cuenta de entrada en el sistema y de la contraseña; si la autentificación tiene éxito, continuar en el Bloque **408**; en otro caso, continuar en el Bloque **407**.

Bloque **407**: El servidor de aplicaciones devuelve un mensaje de fallo de la entrada en el sistema al UE, donde el mensaje de fallo de entrada en el sistema puede contener una razón del fallo.

Bloque **408**: El servidor de aplicaciones envía un mensaje de petición al servidor de PCP, de acuerdo con la información de localización del PCP, solicitando el identificador de asociación almacenado en el PCP del usuario. El mensaje de petición incluye el identificador del usuario e información relevante del servidor de aplicaciones.

Bloque **409**: Tras recibir el mensaje de petición desde el servidor de aplicaciones desde el servidor de aplicaciones, el servidor de PCP interroga a la base de datos para obtener la información de asociación de acuerdo con el identificador del usuario y la información relevante del servidor de aplicaciones, y devuelve el identificador de asociación al servidor de aplicaciones.

Bloque **410**: El servidor de aplicaciones autentifica el identificador de asociación devuelto por el servidor de PCP; si la autentificación tiene éxito, continuar en el Bloque **411**; en otro caso, continuar en el Bloque **412.**

Bloque **411:** El servidor de aplicaciones devuelve un mensaje de fallo de la entrada en el sistema al UE, notificando al usuario que la entrada en el sistema tiene éxito. Y el usuario puede interactuar con el servidor de aplicaciones a través del UE para un servicio específico.

Bloque **412**: El servidor de aplicaciones devuelve un mensaje de fallo de la entrada en el sistema al UE, notificando al usuario que la entrada en el sistema falla. El servidor de aplicaciones puede notificar también al usuario que la razón del fallo es que falla la autentificación del identificador de asociación. La autentificación del identificador de asociación es determinar si el identificador de asociación devuelto por el servidor de PCP es consistente con el identificador de asociación almacenado en el servidor de aplicaciones.

La descripción anterior ilustra un primer modo de realización de la presente invención. Como puede verse por la descripción anterior, en el primer modo de realización de la presente invención, el UE almacena solamente la información de localización del PCP. Y el servidor de aplicaciones solicita el identificador de asociación del usuario, de acuerdo con la información de localización del PCP y autentifica el identificador de asociación.

En modos de realización de la presente invención, el PCP del usuario puede ser almacenado también en el UE. Consecuentemente, cuando se efectúa la autentificación, el UE envía directamente el identificador de asociación del PCP al correspondiente servidor de aplicaciones. El servidor de aplicaciones autentifica el identificador de asociación. El proceso se describe de aquí en adelante en detalle, con referencia a un segundo modo de realización de la presente invención.

El proceso de registro y el proceso de entrada en el sistema del segundo modo de realización de la presente invención, están respectivamente ilustrados en las figuras 5 y 6. Los bloques **501** a **503** del proceso de registro ilustrado en la figura 5 son similares a los bloques **301** a **303** del primer modo de realización. Después de que la autentificación del Bloque **503** haya tenido éxito, continuar en el Bloque **504**.

Bloque **504**: El servidor de PCP envía la información de localización del PCP y el PCP del usuario al UE. El UE almacena la información de localización del PCP y el PCP del usuario. El contenido del PCP puede ser parte de la información relevante de asociación de toda la información relevante de asociación.

Los bloques **505** a **510** son similares a los bloques **305** a **310** y no serán repetidos aquí. En estos bloques, el UE puede enviar la información de localización del PCP al servidor de aplicaciones cuando envíe la petición de registro en el servidor de aplicaciones en el Bloque **505**. El UE puede transportar también la información de localización del PCP del usuario en el acuse que es enviado al servidor de aplicaciones en el Bloque **508,** como respuesta a la

petición sobre si debe asociar el PCP del usuario con la cuenta de servicio.

Bloque **511**: El servidor de PCP actualiza el PCP del usuario. Específicamente, el servidor de PCP añade la información de asociación recibida desde el servidor de aplicaciones al PCP del usuario, y envía una petición de actualización de sincronización del PCP al UE; donde esa petición de actualización de sincronización del PCP contiene la información de asociación.

Bloque **512**: Tras recibir la petición de actualización de sincronización del PCP, el UE añade el identificador de asociación contenido en la petición de actualización de sincronización del PCP al PCP almacenado en el UE, y devuelve un mensaje de sincronización del PCP completada al servidor de PCP.

Bloque **513**: Tras recibir el mensaje de sincronización completada del PCP, el servidor de PCP devuelve un mensaje de éxito de la actualización al servidor de aplicaciones.

El bloque **514** es similar al bloque **316** de la figura 3.

Antes del bloque **511,** es decir, antes de que el servidor de PCP actualice el PCP del usuario, puede haber un bloque adicional para pedir al usuario la determinación, similar a la figura 3. Y al recibir la determinación del usuario, actualizar el PCP del usuario. La implementación detallada tras recibir la determinación del usuario es similar a los bloques **311** a **314** de la figura 3, lo cual no será repetido aquí.

Consecuentemente, en el proceso de entrada en el sistema ilustrado en la figura 6, los bloques **601** a **603** son similares a los bloques **501** a **503** de la figura 5.

Bloque **604**: El servidor de PCP devuelve un mensaje de éxito de la autentificación al UE.

Bloque **605**: El UE envía al servidor de aplicaciones una petición de entrada en el sistema que contiene la cuenta del servicio, el PIN y el identificador de asociación correspondiente al servidor de aplicaciones en el PCP.

Bloque **606**: El servidor de aplicaciones autentifica al usuario de acuerdo con la información recibida incluyendo la autentificación de la cuenta de servicio, del PIN y del identificador de asociación. Si la autentificación tiene éxito, continuar en el bloque **607;** en otro caso, continuar en el bloque **608.**

Bloque **607**: El servidor de aplicaciones devuelve un mensaje de éxito de la entrada en el sistema al UE.

Bloque **608**: El servidor de aplicaciones devuelve un mensaje de fallo de la entrada en el sistema al UE.

En el primer y segundo modos de realización anteriores, cuando el usuario entre en el servidor de aplicaciones, el servidor de aplicaciones autentifica el identificador de asociación. En modos de realización de la presente invención, la autentificación del identificador de asociación puede ser realizada también por el servidor de PCP, lo cual será descrito en detalle con referencia al tercer modo de realización de aquí en adelante.

El proceso de registro del tercer modo de realización es similar al del primer modo de realización. El proceso de entrada en el sistema del tercer modo de realización está ilustrado en la figura 7. Los bloques **701** a **707** son similares a los bloques **401** a **407** de la figura 4. En el bloque **706,** después de que la autentificación de la cuenta de servicio y del PIN haya tenido éxito, continuar en el bloque **708.**

Bloque **708:** El servidor de aplicaciones envía al servidor de PCP una petición de autentificación que contiene el identificador de asociación almacenado en el servidor de aplicaciones, el identificador del usuario y la información del servidor de aplicaciones.

Bloque **709**: El servidor de PCP busca el PCP del usuario de acuerdo con el identificador del usuario y determina si el PCP del usuario contiene un identificador de asociación consistente con el contenido en la petición de autentificación. Si el PCP del usuario contiene un identificador de asociación consistente con el contenido en la petición de autentificación, esta autentificación tiene éxito y se continúa en el bloque **710**; en otro caso, la autentificación falla y se continúa en el bloque **712**.

Bloque **710**: El servidor de PCP devuelve un mensaje de éxito de la autentificación al servidor de aplicaciones.

Bloque **711**: El servidor de aplicaciones devuelve un mensaje de éxito de la entrada en el sistema al UE.

Bloque **712**: El servidor de PCP devuelve un mensaje de fallo de la autentificación al servidor de aplicaciones.

Bloque **713**: El servidor de aplicaciones devuelve un mensaje de fallo de la autentificación al UE.

En el primer a tercer modos de realización anteriores, el identificador de asociación utilizado para asociar el PCP con la cuenta de servicio del usuario, es estático. Para asegurar mejor la seguridad del identificador de asociación, el identificador de asociación puede ser actualizado constantemente, es decir, se puede generar el identificador de

asociación dinámicamente. Se ofrece un cuarto modo de realización de la presente invención para ilustrar la protección de la cuenta de servicio por medio del identificador de asociación dinámico.

En el cuarto modo de realización, el proceso de registro de la cuenta de servicio es similar a los tres anteriores modos de realización. El proceso de entrada en el sistema del cuarto modo de realización difiere de los tres modos de realización anteriores en que: después de que el servidor de aplicaciones devuelva el mensaje de éxito de entrada en el sistema al UE, notificando al usuario de que la entrada en el sistema que utiliza la cuenta de servicio tiene éxito, el servidor de aplicaciones elimina el identificador de asociación correspondiente a la cuenta de servicio, o fija el identificador de asociación correspondiente a la cuenta de servicio como inválido. El servidor de aplicaciones genera un nuevo identificador de asociación utilizado para la autentificación para la próxima vez que el usuario entra en el sistema, y envía una petición de actualización al servidor de PCP solicitando al servidor de PCP que actualice el identificador de asociación. Después de recibir la petición de actualización, el servidor de PCP actualiza el identificador de asociación correspondiente al servidor de aplicaciones, y devuelve un mensaje de éxito de la actualización al servidor de aplicaciones.

Si el PCP del usuario se almacena en el UE, se requiere del servidor de PCP o del servidor de aplicaciones que envíen el nuevo identificador de asociación al UE. El UE actualiza el identificador de asociación almacenado en el UE. El servidor de aplicaciones puede enviar el nuevo identificador de asociación al servidor de PCP y al UE simultáneamente. Después, el servidor de PCP y el UE actualizan respectivamente el identificador de asociación. El servidor de aplicaciones puede enviar también solamente el nuevo identificador de asociación al UE. Después, el UE notifica al servidor de PCP que actualice el identificador de asociación correspondiente al servidor de aplicaciones.

En el cuarto modo de realización, la actualización del identificador de asociación es provocada por un evento de éxito en la entrada al sistema. En modos de realización de la presente invención, la actualización del identificador de asociación puede ser provocada también por otros eventos, por ejemplo, un evento de petición de actualización enviado por el usuario, tras recibir el mensaje de éxito de entrada en el sistema. Además, en modos de realización de la presente invención, la actualización del identificador de asociación puede ser realizada por medio de los dos esquemas siguientes.

El primer esquema es un esquema de actualización provocado por el tiempo. En el primer esquema, se fija por anticipado un tiempo o vida del identificador de asociación. Cuando llega el tiempo de actualización o expira la vida, el servidor de aplicaciones provoca la actualización del identificador de asociación, y actualiza el identificador de asociación en el servidor de PCP o actualiza el identificador de asociación tanto en el servidor de PCP como en el UE. La actualización detallada es similar a la descrita en el cuarto modo de realización y no será repetida aquí. Los identificadores de asociación correspondientes a distintos servicios pueden ser fijados con distintas prioridades. Consecuentemente, el tiempo de actualización y la vida del identificador de asociación pueden ser fijados con distintos valores de acuerdo con la prioridad del identificador de asociación. Por ejemplo, cuanto mayor es la prioridad del identificador de asociación, más corto será el tiempo de actualización y la vida del identificador de asociación. Cuanto menor es la prioridad del identificador de asociación, mayor será el tiempo de actualización y la vida del identificador de asociación.

El segundo esquema es un esquema combinado de actualización por tiempo y evento. El segundo esquema combina el esquema provocado por tiempo y el esquema provocado por un evento. Por ejemplo, después de que transcurra el tiempo de actualización o expire la vida, se actualiza el identificador de asociación y se registra el tiempo de actualización. Después de que suceda un evento tal como que el usuario entre con éxito en el sistema o que el servidor de aplicaciones reciba la petición de actualización desde el UE, se determina si el intervalo de tiempo entre la última actualización y la hora actual excede de un mínimo periodo de actualización. Si el intervalo de tiempo excede del periodo mínimo de actualización, se actualiza el identificador de asociación; en otro caso, no se actualiza el identificador de asociación. En las aplicaciones prácticas, otros tiempos y eventos pueden ser también los que provoquen la actualización del identificador de asociación, lo cual no será descrito aquí.

La descripción anterior es la de los modos de realización preferidos de la presente invención y no debe usarse como limitativa del alcance de la misma. Todas las modificaciones, sustituciones equivalentes o mejoras en el ámbito de la presente invención, estarán incluidas en el ámbito de protección de la presente invención.

REIVINDICACIONES

1. Un método para proteger una cuenta de servicio, que comprende:

autentificar la información de asociación cuando un usuario entra en un servidor de aplicaciones con una cuenta de servicio a través de un Equipo de Usuario UE; si la autentificación tiene éxito, permitir al usuario entrar en el servidor de aplicaciones; en otro caso, rechazar al usuario para que no entre en el servidor de aplicaciones;

donde la información de asociación para la cuenta de servicio del usuario está configurada en un Perfil Personal de Comunicaciones PCP del usuario en un lado de la red,

donde dicho paso de autentificación comprende determinar por el servidor de aplicaciones si la información de asociación configurada en el PCP del usuario es consistente con la información de asociación almacenada en el servidor de aplicaciones.

2. El método de la reivindicación 1, en el que la información de asociación de configuración de la cuenta de servicio del usuario, en el PCP del usuario en el lado de la red, comprende:

generar y almacenar, por el servidor de aplicaciones, la información de asociación cuando el usuario registra la cuenta de servicio en el servidor de aplicaciones, y enviar la información de asociación generada al dispositivo de almacenamiento del PCP para su almacenamiento.

3. El método de la reivindicación 2, que comprende además:

generar, por el servidor de aplicaciones, nueva información de asociación, enviar la nueva información de asociación al dispositivo de almacenamiento del PCP y solicitar al dispositivo de almacenamiento de PCP que actualice la información de asociación;

actualizar, por el dispositivo de almacenamiento del PCP, la información de asociación con la nueva información de asociación;

donde el servidor de aplicaciones genera la nueva información de asociación en cualquiera de los casos siguientes: después de que el servidor de aplicaciones permita al usuario entrar en el sistema; después de que el usuario entre con éxito en el sistema y el servidor de aplicaciones reciba una petición de actualización desde el usuario; después de que expire un temporizador para actualizar la información de asociación; después de que expire el tiempo de vida de la información de asociación; después de que el usuario entre con éxito en el sistema y el servidor de aplicaciones reciba una petición de actualización desde el usuario y el intervalo de tiempo entre el tiempo en el que el servidor de aplicaciones recibe la petición de actualización y el tiempo de la última actualización, sea mayor que un periodo mínimo de actualización.

4. El método de la reivindicación 2, que comprende además:

enviar, por el dispositivo de almacenamiento del PCP, antes de almacenar la información de asociación en el PCP del usuario, un mensaje de aviso al UE para avisar al usuario si debe asociar la cuenta de servicio del usuario con el PCP del usuario; y

recibir, por el dispositivo de almacenamiento del PCP, un acuse desde el UE.

5. El método de la reivindicación 2, que comprende además:

enviar, por el servidor de aplicaciones, un mensaje de interrogación al UE para interrogar al usuario sobre si debe asociar la cuenta de servicio del usuario con el PCP del usuario;

recibir, por el servidor de aplicaciones, un acuse desde el UE.

6. El método de la reivindicación 2, en el que la autentificación de la información de asociación comprende:

enviar, por el servidor de aplicaciones, una petición al dispositivo de almacenamiento del PCP, solicitando la información de asociación para la cuenta de servicio;

obtener, por el servidor de aplicaciones, la información de asociación desde el dispositivo de almacenamiento del PCP; y

determinar, por el servidor de aplicaciones, si la información de asociación recibida desde el dispositivo de almacenamiento del PCP es consistente con la información de asociación almacenada en el servidor de aplicaciones.

7. El método de la reivindicación 2, en el que la autentificación de la información de asociación comprende:

enviar, por el servidor de aplicaciones, tras recibir una petición de entrada en el sistema desde el UE, la información de asociación para la cuenta de servicio almacenada en el servidor de aplicaciones, al dispositivo de almacenamiento del PCP; y

determinar, por el dispositivo de almacenamiento del PCP, si el PCP del usuario comprende información de asociación consistente con la información de asociación recibida desde el servidor de aplicaciones, para obtener un resultado de la autentificación; y devolver el resultado de la autentificación al servidor de aplicaciones.

8. El método de la reivindicación 6 o 7, que comprende además:

enviar, por el dispositivo de almacenamiento del PCP, información de localización del PCP del usuario al UE;

recibir, por el servidor de aplicaciones, la información de localización del PCP desde el UE; e

interactuar, por el servidor de aplicaciones, con el dispositivo de almacenamiento del PCP, de acuerdo con la información de localización del PCP del usuario.

9. El método de la reivindicación 2, que comprende:

enviar, por el dispositivo de almacenamiento del PCP, la información de asociación del PCP del usuario al UE;

recibir, por el servidor de aplicaciones, la información de asociación desde el UE; y

la autentificación de la información de asociación comprende:

determinar, por el servidor de aplicaciones, si la información de asociación recibida desde el UE es consistente con la información de asociación almacenada en el servidor de aplicaciones.

10. El método de la reivindicación 9, que comprende además:

enviar, por el dispositivo de almacenamiento del PCP, una petición de sincronización al UE, solicitando que actualice la información de asociación almacenada en el UE, cuando el dispositivo de almacenamiento del PCP actualiza la información de asociación del usuario.

11. Un sistema para proteger una cuenta de servicio, que comprende:

un servidor de aplicaciones, adaptado para interactuar con un dispositivo de almacenamiento del Perfil Personal de Comunicaciones PCP y un Equipo de Usuario UE basándose en una petición de entrada en el sistema de un usuario, autentificar la información de asociación en el PCP del usuario, y permitir que el usuario entre en el servidor de aplicaciones si la autentificación tiene éxito;

donde el dispositivo de almacenamiento del PCP está adaptado para almacenar el PCP del usuario; donde el PCP contiene información de asociación para la cuenta de servicio del usuario; donde dicho paso de autentificación comprende determinar, por el servidor de aplicaciones, si la información de asociación configurada en el PCP del usuario es consistente con la información de asociación almacenada en el servidor de aplicaciones.

12. El sistema de la reivindicación 11, en el que el servidor de aplicaciones está adaptado además para generar y almacenar la información de asociación de la cuenta de servicio del usuario, tras recibir una petición de registro, y enviar la información de asociación generada al dispositivo de almacenamiento del PCP.

13. El sistema de la reivindicación 11 o 12, donde el servidor de aplicaciones está adaptado además para recibir información de localización del PCP desde el UE, a través de una petición de entrada en el sistema: y para enviar una petición al dispositivo de almacenamiento del PCP para solicitar la información de asociación para la cuenta de servicio del usuario, de acuerdo con la información de localización del PCP de la petición de entrada en el sistema; y determinar si la información de asociación recibida desde el dispositivo de almacenamiento del PCP es consistente con la información de asociación almacenada en el servidor de aplicaciones;

el dispositivo de almacenamiento del PCP está adaptado además para enviar la información de localización del PCP del usuario al UE, y enviar la información de asociación para la cuenta de servicio del usuario al servidor de aplicaciones, como respuesta a la petición del servidor de aplicaciones.

14. El sistema de la reivindicación 13, donde el servidor de aplicaciones está adaptado además para eliminar la información de asociación almacenada en el servidor de aplicaciones o para fijar la información de asociación almacenada en el servidor de aplicaciones como inválida, después de que la autentificación haya tenido éxito, generar nueva información de asociación para la cuenta de servicio del usuario, y enviar la nueva información de asociación al dispositivo de almacenamiento del PCP;

el dispositivo de almacenamiento del PCP está adaptado además para actualizar la información de asociación

almacenada en el dispositivo de almacenamiento del PCP, de acuerdo con la nueva información de asociación recibida desde el servidor de aplicaciones.

15. El sistema de la reivindicación 11 o 12, en el que el dispositivo de almacenamiento del PCP está adaptado además para enviar la información de asociación almacenada en el dispositivo de almacenamiento del PCP al UE;

el servidor de aplicaciones está adaptado además para recibir la información de asociación transportada en la petición de entrada en el sistema desde el UE; y determinar si la información de asociación transportada en la petición de entrada en el sistema es consistente con la información de asociación almacenada en el servidor de aplicaciones, y devolver un mensaje de éxito de la entrada en el sistema o un mensaje de fallo de la entrada en el sistema al UE.

16. El sistema de la reivindicación 15, que comprende además un Equipo de Usuario UE, donde el servidor de aplicaciones está adaptado además para eliminar la información de asociación almacenada en el servidor de aplicaciones o fijar la información de asociación almacenada en el servidor de aplicaciones como inválida, después de que la autentificación haya tenido éxito; generar nueva información de asociación para la cuenta de servicio del usuario, y enviar la nueva información de asociación al dispositivo de almacenamiento del PCP y al UE;

el dispositivo de almacenamiento del PCP está adaptado también para actualizar la información de asociación almacenada en el dispositivo de almacenamiento del PCP, de acuerdo con la nueva información de asociación recibida desde el servidor de aplicaciones;

el UE está adaptado también para actualizar la información de asociación almacenada en el UE, de acuerdo con la nueva información de asociación recibida desde el servidor de aplicaciones.

17. El sistema de la reivindicación 15, que comprende además un Equipo de Usuario UE, donde el servidor de aplicaciones está adaptado además para eliminar la información de asociación almacenada en el servidor de aplicaciones o para fijar la información de asociación almacenada en el servidor de aplicaciones como inválida, después de devolver el mensaje de éxito de entrada en el sistema al UE; generar nueva información de asociación para la cuenta de servicio del usuario y enviar la nueva información de asociación al UE;

el UE está adaptado también para actualizar la información de asociación almacenada en el UE, de acuerdo con la nueva información de asociación recibida desde el servidor de aplicaciones, devolver un mensaje de éxito de la actualización al servidor de aplicaciones, y enviar la nueva información de asociación al servidor de almacenamiento del PCP;

el dispositivo de almacenamiento del PCP está adaptado también para actualizar la información de asociación almacenada en el dispositivo de almacenamiento del PCP, de acuerdo con la nueva información de asociación recibida desde el UE.

18. El sistema de la reivindicación 11, en el que el dispositivo de almacenamiento del PCP comprende cualquiera entre un servidor de PCP, un servidor de ficheros de UE y una base de datos de UE.

19. El sistema de la reivindicación 11, en el que el servidor de aplicaciones adaptado para la autentificación de la información de asociación comprende además:

enviar la información de asociación y devolver un mensaje de éxito de entrada en el sistema o un mensaje de fallo de entrada en el sistema al UE; donde la información de asociación está configurada para una cuenta de servicio del usuario y está almacenada en un Perfil Personal de Comunicaciones PCP del usuario;

donde el dispositivo de almacenamiento del PCP está adaptado además para autentificar la información de asociación recibida desde el servidor de aplicaciones y devolver un mensaje de éxito de la autentificación o un mensaje de fallo de la autentificación al servidor de aplicaciones.

20. El sistema de la reivindicación 19, en el que el servidor de aplicaciones está adaptado además para generar y almacenar la información de asociación después de recibir una petición de registro desde el UE, y enviar la información de asociación al dispositivo de almacenamiento del PCP; y

el dispositivo de almacenamiento del PCP está adaptado además para almacenar la información de asociación recibida desde el servidor de aplicaciones.

21. El sistema de la reivindicación 20, en el que el servidor de aplicaciones está adaptado además para eliminar la información de asociación almacenada en el servidor de aplicaciones o para fijar la información de asociación como inválida después de que la autentificación haya tenido éxito; generar nueva información de asociación para la cuenta de servicio del usuario, y enviar la nueva información de asociación al dispositivo de almacenamiento del PCP;

el dispositivo de almacenamiento del PCP está adaptado además para actualizar la información de asociación almacenada en el dispositivo de almacenamiento del PCP, de acuerdo con la nueva información de asociación recibida desde el servidor de aplicaciones, y devolver un mensaje de éxito de la actualización al servidor de aplicaciones.

22. Un dispositivo para almacenar un Perfil Personal de Comunicaciones PCP de un usuario, que comprende:

una base de datos de PCP, adaptada para almacenar un PCP de un usuario y la información de asociación de una cuenta de servicio del usuario;

una unidad de autentificación adaptada para recibir la información de asociación; determinar si la base de datos PCP comprende información de asociación consistente con la información de asociación recibida, y devolver un mensaje de éxito de la autentificación o un mensaje de fallo de la autentificación.

23. El dispositivo de la reivindicación 22, que comprende además:

una unidad de pasarela de acceso a servicio abierto, adaptada para conectar comunicativamente la unidad de autentificación con el servidor de aplicaciones;

una unidad de interfaz a componentes de servicio, adaptada para conectar comunicativamente la unidad de autentificación.

24. El dispositivo de la reivindicación 22, en el que la base de datos de PCP está adaptada además para actualizar la información de asociación almacenada en la base de datos de PCP, de acuerdo con la nueva información de asociación recibida desde un servidor de aplicaciones.

25. Un servidor de aplicaciones para proteger una cuenta de servicio de un usuario, que comprende: una unidad de control de la entrada en el sistema y una unidad de comunicaciones; donde

la unidad de control de la entrada en el sistema está adaptada para recibir una petición de entrada en el sistema a través de la unidad de comunicaciones; solicitar la información de asociación basada en la información de localización del PCP del usuario, contenida en la petición de entrada en el sistema; determinar si la información de asociación recibida es consistente con la información de asociación almacenada en la unidad de control de entrada en el sistema; y enviar un mensaje de éxito de la entrada en el sistema o un mensaje de fallo de la entrada en el sistema, a través de la unidad de comunicaciones.

26. El servidor de aplicaciones de la reivindicación 25, en el que la unidad de control de entrada en el sistema está adaptada además para eliminar la información de asociación almacenada en la unidad de control de entrada en el sistema o para fijar como inválida la información de asociación almacenada en la unidad de control de entrada en el sistema, después de que la autentificación haya tenido éxito; generar nueva información de asociación para la cuenta de servicio del usuario, y enviar la nueva información de asociación.

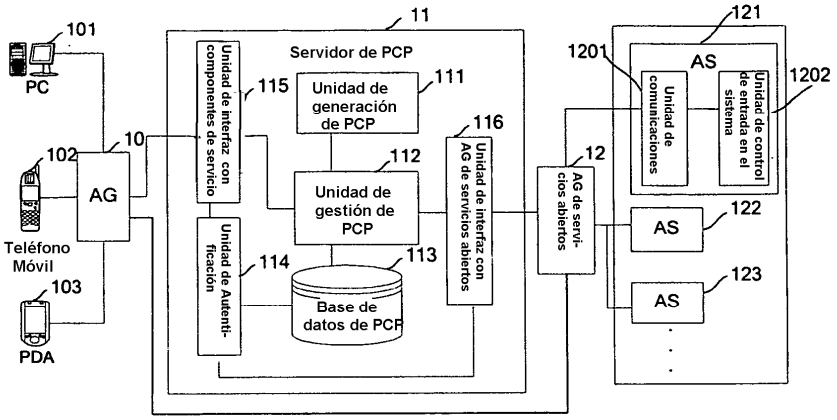

Figura 1

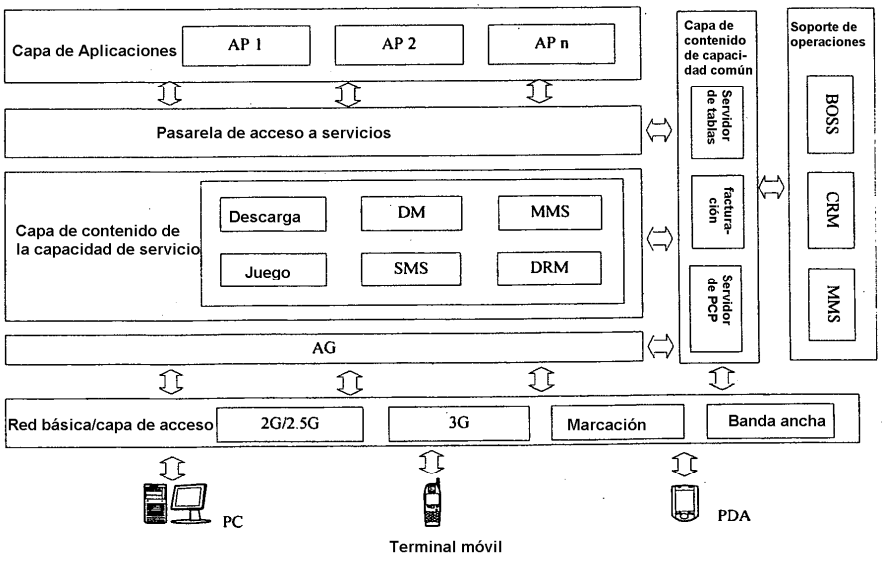

Figura 2

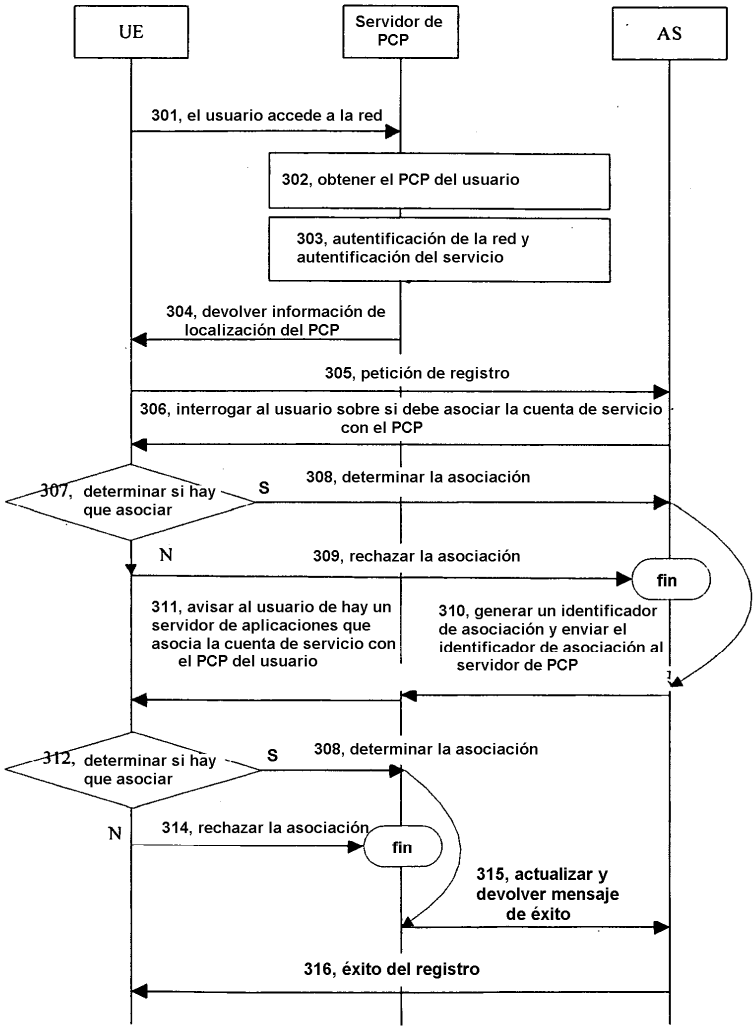
UE
Servidor de PCP
AS
301, el usuario accede a la red
302, obtener el PCP del usuario
303, autentificación de la red y autentificación del servicio
304, devolver información de localización del PCP
305, petición de registro
306, interrogar al usuario sobre si debe asociar la cuenta de servicio con el PCP
307, determinar si hay que asociar
S
308, determinar la asociación
N
309, rechazar la asociación
fin
311, avisar al usuario de hay un servidor de aplicaciones que asocia la cuenta de servicio con el PCP del usuario
310, generar un identificador de asociación y enviar el identificador de asociación al servidor de PCP
312, determinar si hay que asociar
S
308, determinar la asociación
N
314, rechazar la asociación
fin
315, actualizar y devolver mensaje de éxito
316, éxito del registro

Figura 3

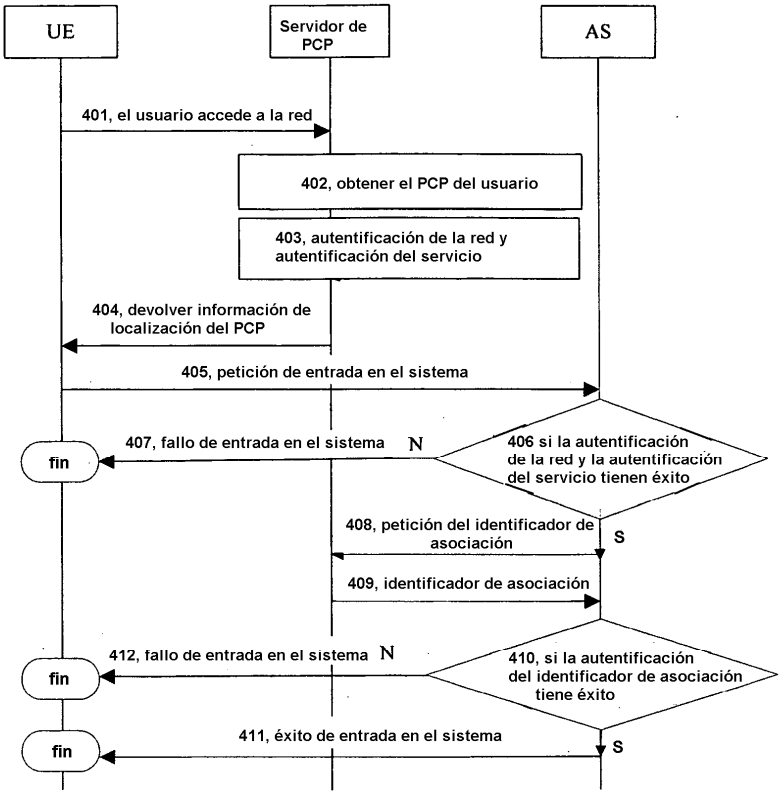
UE
Servidor de PCP
AS
401, el usuario accede a la red
402, obtener el PCP del usuario
403, autentificación de la red y autentificación del servicio
404, devolver información de localización del PCP
405, petición de entrada en el sistema
406 si la autentificación de la red y la autentificación del servicio tienen éxito
407, fallo de entrada en el sistema
N
fin
S
408, petición del identificador de asociación
409, identificador de asociación
410, si la autentificación del identificador de asociación tiene éxito
412, fallo de entrada en el sistema
N
fin
411, éxito de entrada en el sistema
S
fin

Figura 4

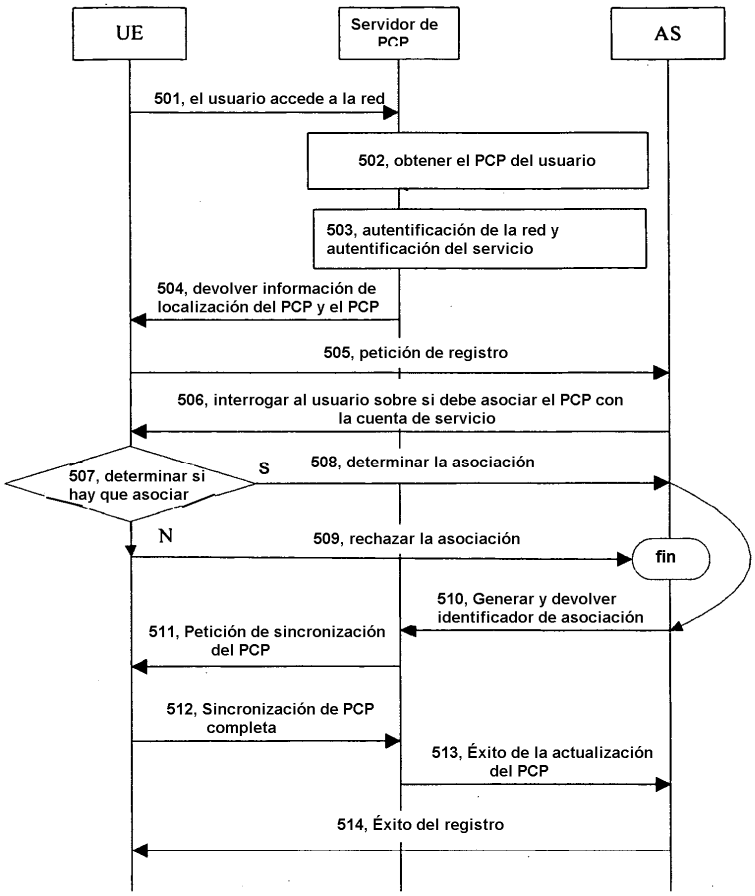
UE
Servidor de PCP
AS
501, el usuario accede a la red
502, obtener el PCP del usuario
503, autentificación de la red y autentificación del servicio
504, devolver información de localización del PCP y el PCP
505, petición de registro
506, interrogar al usuario sobre si debe asociar el PCP con la cuenta de servicio
507, determinar si hay que asociar
S
508, determinar la asociación
N
509, rechazar la asociación
fin
510, Generar y devolver identificador de asociación
511, Petición de sincronización del PCP
512, Sincronización de PCP completa
513, Éxito de la actualización del PCP
514, Éxito del registro

Figura 5

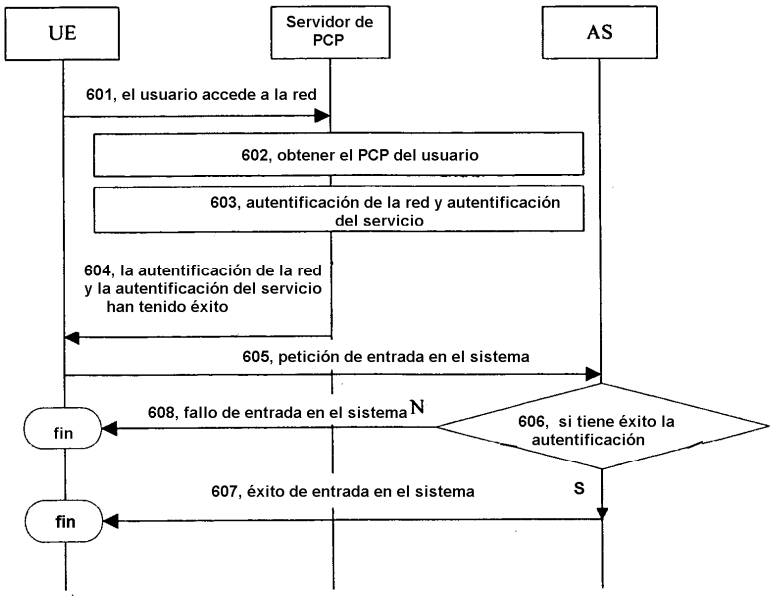
UE
Servidor de PCP
AS
601, el usuario accede a la red
602, obtener el PCP del usuario
603, autentificación de la red y autentificación del servicio
604, la autentificación de la red y la autentificación del servicio han tenido éxito
605, petición de entrada en el sistema
606, si tiene éxito la autentificación
N
608, fallo de entrada en el sistema
fin
S
607, éxito de entrada en el sistema
fin

Figura 6

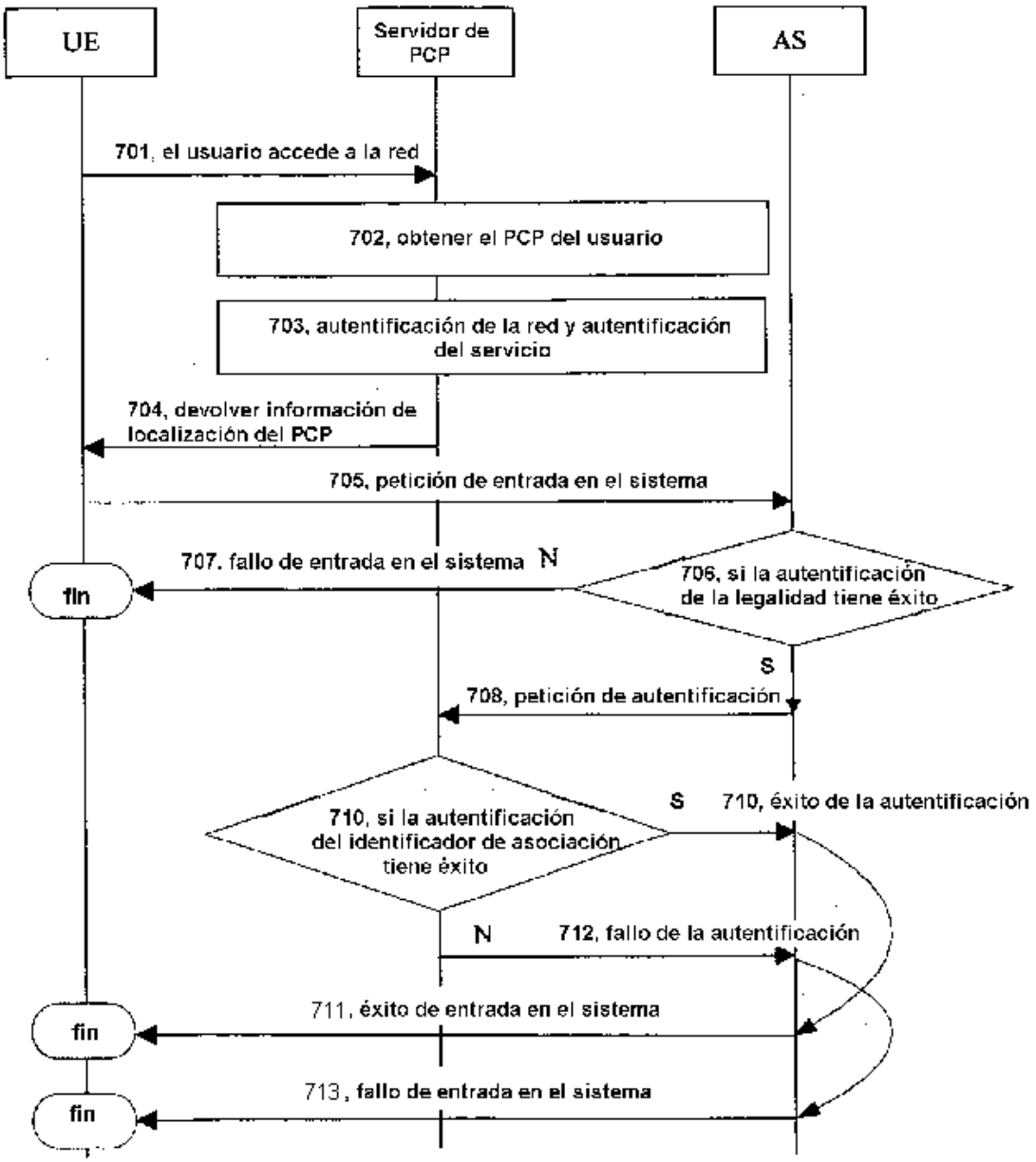
UE
Servidor de PCP
AS
701, el usuario accede a la red
702, obtener el PCP del usuario
703, autentificación de la red y autentificación del servicio
704, devolver información de localización del PCP
705, petición de entrada en el sistema
706, si la autentificación de la legalidad tiene éxito
N
707. fallo de entrada en el sistema
fin
S
708, petición de autentificación
710, si la autentificación del identificador de asociación tiene éxito
S
710, éxito de la autentificación
N
712, fallo de la autentificación
711, éxito de entrada en el sistema
fin
713, fallo de entrada en el sistema
fin

Figura 7