(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 371 109**

(51) Int. CI.:
H04W 8/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07720803 .1**
(96) Fecha de presentación: **16.04.2007**
(97) Número de publicación de la solicitud: **2009934**
(97) Fecha de publicación de la solicitud: **31.12.2008**

(54) Título: **SISTEMA Y APARATO PARA USUARIOS DE CS MÓVIL PARA ACCEDER A LA RED DE IMS Y EL MÉTODO DE REGISTRO PARA EL ACCESO.**

(30) Prioridad:
20.04.2006 CN 200610075931

(45) Fecha de publicación de la mención BOPI:
27.12.2011

(45) Fecha de la publicación del folleto de la patente:
27.12.2011

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

(72) Inventor/es:
ZHU, Dongming y
LI, Yan

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

DESCRIPCIÓN

Sistema y aparato para usuarios de CS móvil para acceder a la red de IMS y el método de registro para el acceso

CAMPO DE LA INVENCIÓN

La presente invención se refiere a tecnologías de las comunicaciones y en particular, a una tecnología para un usuario no de un Subsistema Multimedia de IP (IMS) para acceder a una red IMS.

ANTECEDENTES DE LA INVENCIÓN

La Red Móvil Pública Terrestre (PLMN) definida por el Proyecto de Asociación de Tercera Generación (3GPP) se puede dividir lógicamente en dos partes: una Red de Núcleo (CN) y una Red de Acceso (AN). La red CN se puede subdividir, a su vez, en un dominio de Circuitos Conmutados (CS), un dominio de Paquetes Conmutados (PS) y un subsistema IMS. En una CN diferente, un usuario debe utilizar un modo de acceso diferente.

(i) dominio de CS y acceso del usuario

El dominio de CS proporciona servicios de CS para usuarios, incluyendo voz, datos de CS y fax. Entidades típicas del dominio de CS comprenden: un Centro de Conmutación para Móviles (MSC), adaptado para gestionar la señalización de llamadas y concluir el encaminamiento de llamadas; una Pasarela Multimedia Inalámbrica (WMG), adaptada para establecer conexiones multimedia y convertir códigos de voz; un Registro de Posición de Visitantes (VLR), adaptado para almacenar información sobre la posición actual de un usuario y los datos de servicios; un Registro de Posición Base (HLR), adaptado para almacenar datos de suscripción de un usuario y la información sobre el VLR en servicio actual; un Registro de Identidad de Equipo (EIR), adaptado para almacenar identidades de equipos de usuarios y un Centro de Autenticación (AuC), adaptado para generar datos de autenticación.

Para garantizar que los servicios en el dominio de CS sean accesibles a los usuarios, el protocolo 3GPP define un mecanismo para un usuario de CS móvil para acceder a una red CN. Mediante este mecanismo, la red puede obtener la información de posición del usuario y poner en práctica la protección de seguridad de acceso a la red.

La red necesita gestionar las peticiones de acceso cuando un usuario de CS móvil activa un Equipo Móvil (ME), realiza una itinerancia a una nueva área de servicios de MSC/VLR, actualiza la posición periódicamente o factura un servicio.

Un operador de red puede decidir utilizar o no utilizar algunos procesos relacionados con el acceso, por ejemplo, proceso de autenticación, proceso de encriptación, proceso de asignación de una Identidad de Abonado Móvil Temporal (TMSI), en diferentes operaciones de acceso en conformidad con políticas específicas.

Un proceso de acceso típico de un usuario de 3G CS se representa en la Figura 1. Un equipo móvil (ME) envía una petición de actualización de posición al Controlador de Red de Radio (RNC) y envía una petición de información de autenticación al HLR/AUC a través de un MSC/VLR, por turno; en adelante, el HLR/AUC reenvía un mensaje de petición de autenticación al MSC/VLR, RNC y ME, por turno.

El proceso para un usuario de CS para acceder a una red comprende, además, un proceso de iniciación de protección de seguridad.

Las identidades para uso en un proceso de acceso de un usuario de CS comprenden: Número de ISDN de Abonado Móvil (MSISDN), Identidad Internacional del Abonado a un Móvil (IMSI) y TMSI. La composición de una identidad IMSI se representa en la Figura 2. Una IMSI identifica inequívocamente un usuario en una red móvil global y está vinculada al número MSISDN del usuario en el momento de la suscripción.

Según se indica en la Figura 2, una identidad IMSI consiste en tres partes: Código de País del Móvil (MCC), Código de Red Móvil (MNC) y Número de Identificación de Abonado al Móvil (MSIN). El código MCC es promulgado por la ITU-T y se aplica de forma global. Un MNC se asigna por el país que rige el MCC en función de las condiciones reales y se expresa por dos o tres dígitos. Un MSIN se asigna por un operador que mantiene el MCC y el MNC. Una Identidad Nacional de Abonado a Móvil (NMSI) se expresa como “MNC + MSIN”.

Según se representa en la Figura 3, un número MSISDN se asigna en conformidad con el plan de numeración de ITU E.164 y especificaciones de E.213 y consiste en tres partes: Código de País (CC), Código Nacional de Destino (NDC) y Número de Identificación de Abonado a Móvil (MSIN). Un código CC es un código de área de peaje internacional y se promulga por la ITU-T y se aplica de forma global. Un NDC se define por el país que rige el CC y se asigna en función de las condiciones del país. Un operador móvil puede disponer de más de un NDC, por ejemplo, 135–139 mantenido por China Mobile y 130–134 mantenido por China Unicom. Un número nacional se define por el operador que mantiene “CC + NDC”. Un número nacional se expresa como “NDC + SN”.

Un número MSISDN debe ser capaz de servir como un Título Global (GT) de la Parte de Control de Conexión de Señalización (SCCP) para localizar el HLR del usuario. En el proceso de direccionamiento, el HLR, que sirve al usuario, puede estar situado según el "CC + NDC" del número o, como opción, más la parte del número de abonado (SN). La identidad del HLR relacionado con el registro del usuario puede ser un número HLR que cumpla las especificaciones de E.164 o un identificador HLR ID. El formato de un número de HLR es el mismo que el de un MSISDN. Un HLR ID consiste en varias partes de una IMSI, a saber, los primeros dígitos de "MCC + MNC + MSIN".

La TMSI es una identidad efectiva, al nivel local, en el área de servicios de MSC/VLR. Se utiliza con una Identidad de Área de Posición (LAI). Por lo tanto, el operador de red puede estipular que una TMSI debe reasignarse para cada acceso. Para evitar que un eavesdropper ('escuchante furtivo') determine la posición del usuario a través de un identificador ID único, la red de GSM/WCDMA suele asignar una TMSI al usuario que accede inicialmente a un área de servicios de MSC/VLR.

El usuario de CS que accede a la red debe ser objeto de autenticación. El proceso de autenticación comprende: la obtención de un vector de autenticación (AV) mediante el MSC/VLR (MSC está combinado con VLR) y la realización de una autenticación bidireccional con el usuario.

El proceso para un MSC/VLR para obtener un vector AV comprende: cuando un MSC/VLR de la red CN recibe una petición de actualización de posición de usuario para acceso, si el MSC/VLR determina que el usuario necesita autenticación, el MSC/VLR solicita un AV desde el HLR/AUC (HLR está combinado con AUC). El AUC genera varios grupos de vectores AVs dispuestos, de forma secuencial, en función de la IMSI del usuario. Un AV comprende cinco elementos (RAND, AUTN, CK, IK, RES). El HLR reenvía todos los vectores AVs generados al MSC/VLR mediante una respuesta.

Después de obtener un vector AV, el MSC/VLR realiza un proceso de autenticación bidireccional con el usuario que comprende: después de recibir los grupos de AV, el MSC/VLR selecciona un AV intacto, elimina la respuesta (RES) y la envía al RNC para requerir la iniciación de la autenticación. El RNC elimina la clave de cifrado (CK) y la clave de integridad (IK) de los vectores AVs restantes y envía una petición de autenticación al ME (USIM). El USIM, en el ME, puede calcular las CK, IK y RES en el grupo de AV utilizando diferentes algoritmos compartidos con la red en función de la clave (K) que se asigna en el momento de la suscripción y es compartida en el AUC de la red así como el número aleatorio recibido (RAND). En función del número RAND, el denominado *token* de autenticación (AUTN) y la clave compartida (K), el ME calcula el MAC y compara el valor obtenido con el valor de MAC recibido desde la red AUTN. Si los dos valores son los mismos, el ME reenvía el RES calculado al MSC/VLR. El MSC/VLR compara el valor con el RES almacenado en el AV y, si los dos valores coinciden, determina que el ME supera la autenticación y es legal.

En un sistema de GSM, el proceso de acceso de un usuario de GSM es similar al de un usuario de CS en un sistema 3G, tal como un sistema CDMA. Según se ilustra en la Figura 4, las diferencias entre el proceso de acceso de un usuario de GSM y el de un usuario de 3G CS comprenden:

El sistema de GSM no tiene ningún ME para autenticación de la red, de modo que el vector AV no contiene ningún parámetro de AUTN;

El sistema de GSM no dispone de ninguna protección de integridad de datos, por lo que el AV no contiene ningún parámetro de IK y

Una clave de cifrado (Kc) del sistema de GSM contiene solamente 64 dígitos, mientras que una clave CK, utilizada en el sistema 3G, contiene 128 dígitos y el algoritmo de encriptación aplicado en el sistema de 3G es más intenso.

La respuesta firmada (SRES) de un sistema de GSM difiere de la RES de un sistema de 3G en algoritmo y longitud.

El proceso de acceso de un usuario de sistema 3G y 2G CS, anteriormente descrito, revela que un mecanismo de seguridad se establece para el dominio de CS móvil para proporcionar garantía de seguridad en alguna medida. El mecanismo de seguridad de un usuario de 3G es una mejora del mecanismo de seguridad del usuario de GSM. Es decir, el mecanismo de seguridad de 3G es una evolución suave a partir del mecanismo de seguridad 2G.

Lo que antecede es un proceso de acceso de la red de CS y del usuario de CS. A continuación se describe un proceso de acceso de la red IMS y del usuario de IMS.

El IMS es un subsistema que está sobrepuesto sobre el dominio de PS existente y soporta los servicios multimedia de IP. Está previsto que proporcione servicios multimedia ricos en contenidos, tales como de audio, vídeo, texto, sesión interactiva o sus combinaciones. El IMS utiliza el Protocolo de Iniciación de Sesión (SIP) y es independiente del acceso.

Según se representa en la Figura 5, las entidades funcionales en un IMS comprenden: una entidad de función de Control de Sesión de Llamadas (CSCF) que controla el registro de usuarios y la sesión, un Servidor de Aplicación (AS) que proporciona varias funciones de control lógico del servicio y un Servidor de Abonado Base (HSS) que gestiona los datos de suscripción en conjunto. Un usuario accede al IMS a través del denominado Proxy-CSCF (P-CSCF) de una posición

visitada actual. El CSCF-Servidor (S-CSCF), en el dominio base controla la iniciación operativa de sesiones y servicios e interacciona con el servidor AS acerca del control del servicio.

En una red de IMS, cada usuario que se suscribe al servicio de IMS posee una o más identidades de usuario privado asignadas por el operador de la red base para la finalidad de registro, autorización, gestión y facturación. Cada usuario de IMS posee una o más identidades de usuarios públicos previstas para su uso en los procesos de sesiones de servicios y para identificar el usuario durante la comunicación con otros usuarios.

La Figura 6 representa la suscripción de IMS y la relación entre la identidad de usuario público y la identidad de usuario privado en un IMS. Una identidad de usuario privado corresponde a una o más identidades de usuario público.

En una red IMS, el proceso de acceso de un usuario de IMS se puede dividir en: registro inicial del usuario, re-registro del usuario, de-registro del usuario, re-autenticación iniciada por la red, de-registro iniciado por la red y suscripción de eventos después del registro.

En el registro iniciado por un usuario, estos parámetros se deben transmitir en la petición: una Identidad Pública Multimedia IP (IMPU), una Identidad Privada Multimedia IP (IMPI) y un nombre de dominio base del usuario. Otros parámetros tales como la capacidad de autenticación y la dirección de IP de un Equipo de Usuario (UE) se pueden realizar adicionalmente.

Según se representa en la Figura 7, el proceso de registro inicial iniciado por un usuario de IMS comprende:

El usuario utiliza la IMPU, la IMPI, la dirección de contacto y el nombre de dominio base almacenados en el módulo de ISIM para elaborar un mensaje de Registro de SIP. El mensaje transmite, además, la información sobre el tipo y el ID de la red de acceso del usuario, la encriptación soportada, las opciones de algoritmos de integridad, el puerto requerido para establecer una Asociación de Seguridad (SA) con la P-CSCF y la duración del intervalo de espera. A continuación, el usuario envía el mensaje a la dirección por defecto de la P-CSCF encontrada, con anterioridad, por el UE en el proceso de descubrimiento de la P-CSCF.

Después de recibir el mensaje, la P-CSCF almacena la identidad del usuario y otra información necesaria, consulta la dirección de la CSCF–Interrogador (I-CSCF) del dominio base en función del nombre del dominio base y elabora un nuevo mensaje de Registro que transmite la información sobre la red visitada y envía el mensaje a la dirección de I-CSCF indicada por el resultado de la consulta.

En función de la identidad privada del usuario, la I-CSCF consulta el HSS respecto al estado de registro del usuario. Si el usuario no está registrado, la I-CSCF selecciona una S-CSCF para gestionar la petición de registro del usuario. Después de seleccionar una S-CSCF, la I-CSCF envía la petición de Registro a la S-CSCF para un procesamiento adicional.

Después de recibir el mensaje de Registro, la S-CSCF comprueba y determina que el usuario está inicialmente registrado y solicita al HSS que asigne un vector de autenticación (AV) al usuario. La composición del AV es la misma que la de un AV de usuario 3G y es un vector quintupleto. Después de recibir el resultado de asignación del HSS, la S-CSCF selecciona un grupo de vectores a partir del mensaje de SIP 401, elimina las XRES en los vectores y envía los vectores a la P-CSCF a través de la I-CSCF.

Después de eliminar las claves CK e IK en el vector AV, la P-CSCF selecciona un algoritmo preferido en función de las capacidades de algoritmos de encriptación y de integridad de la P-CSCF y el equipo UE y establece los parámetros de la asociación de seguridad en la P-CSCF. La P-CSCF introduce dichos parámetros en el mensaje 401 e inicia un desafío de autenticación para el UE.

El equipo de usuario UE calcula las CK, IK y RES en función de la Clave de Autenticación (K) compartida con la red y la RAND recibida y realiza la autenticación de la red en la misma manera que en un dominio de 3G CS. A continuación, negocia la asociación de seguridad, en función de los parámetros pertinentes, reenviados por la P-CSCF. Después de la negociación de la asociación de seguridad, la señalización en el UE y el lado de la red utiliza el puerto definido por la asociación de seguridad para la comunicación. Después de calcular la RES requerida por la red, el UE necesita elaborar un nuevo mensaje de Registro. Después de la protección de integridad y encriptación, el mensaje se envía a la P-CSCF a través del canal de seguridad conectado a la P-CSCF.

La función P-CSCF desencripta el mensaje recibido. Si el mensaje se resuelve de forma satisfactoria, la red y el UE han concluido la protección de integridad y encriptación. Más adelante, la P-CSCF envía el resultado de la autenticación a la S-CSCF a través de la I-CSCF. Después de recibir el mensaje de Registro, la S-CSCF compara la RES, en el mensaje, con la RES almacenada con anterioridad. Si son las mismas, la autenticación es satisfactoria. Una vez concluida la autenticación, la S-CSCF notifica al HSS el éxito de la autenticación y descarga los datos de usuarios desde el HSS. A continuación, la S-CSCF envía un mensaje 200 OK al equipo UE, indicando que el registro fue tuvo éxito. El mensaje transmite la duración del registro medida en segundos, que se especifica por la red. Además, la S-CSCF puede iniciar el registro de terceros para el Servidor de Aplicación (AS) especificado en las condiciones de iniciación operativa en función de las condiciones de iniciación en los datos de usuarios.

Después de recibir una respuesta 200 OK, la P-CSCF inicia un proceso de suscripción para el paquete de eventos de registro del UE a la S-CSCF. Una vez que se realiza satisfactoriamente la suscripción, la S-CSCF reenvía el estado de registro a la P-CSCF.

Después de recibir la respuesta de 200 OK, el UE inicia un proceso de suscripción para el paquete de eventos de registro del UE a la S-CSCF. Después de la suscripción satisfactoria, la S-CSCF reenvía el estado de registro al UE.

Después de la conclusión del registro, los siguientes procesos pueden realizarse para un usuario que accede a la red de IMS:

(1) El proceso de re-registro iniciado por el usuario se representa en la Figura 8. Antes de terminar la duración del registro, el equipo UE inicia un re-registro para la red e indica el soporte de la protección de integridad a la red. Según se representa en la Figura, la S-CSCF juzga si hay que re-autenticar al usuario o no. Si no se requiere ninguna autenticación, la S-CSCF reenvía una respuesta 200 OK al UE.

(2) El proceso del de-registro, iniciado por el usuario, consiste en: en el mensaje de Registro, el UE pone “expira” (un parámetro que indica la duración del registro) a 0. La S-CSCF notifica al HSS que el usuario está de-registrado. Si el UE no tiene otras condiciones de iniciación operativa del estado no registrado, la S-CSCF ya no almacenará información sobre el usuario.

(3) Según se representa en la Figura 9, el proceso de re-registro iniciado por una red de IMS comprende:

La S-CSCF, en la red, inicia el re-registro del UE. El re-registro ha de enviar un mensaje SIP NOTIFY al equipo UE. Después de que el usuario inicie el re-registro, la red decide si hay que re-autenticar, o no, al usuario en función de la política operativa.

Después de enviar un mensaje NOTIFY, la S-CSCF aporta la duración del registro de la IMPI correspondiente del usuario. En este periodo, si el UE no inicia ningún proceso de re-registro, la S-CSCF inicia un proceso de de-registro.

(4) El proceso de de-registro, iniciado por la red IMS, se representa en la Figura 10. Cuando los datos de usuario se suprimen del HSS o se inicia un de-registro por un evento interno (intervalo de espera del temporizador de re-registro) de la función S-CSCF, la red de IMS inicia un proceso de de-registro. En el proceso de de-registro, diferentes parámetros se transmiten en el mensaje NOTIFY, dependiendo de si la red de IMS espere, o no, que el UE inicie de nuevo el registro.

Con el desarrollo de las tecnologías de comunicaciones de redes, la integración de una red de IMS con una red de CS se convierte en una megatendencia en el sector. Para cumplir los requisitos de aplicación de multimedia de IP cada vez más estrictos, el protocolo 3GPP propone un IMS de una arquitectura de red de servicios de todo IP, sobre la base de una red de soporte de paquetes. La red integrada está prevista para proteger el modo de acceso del usuario y mejorar la experiencia de comunicación multimedia. Por lo tanto, se requiere una solución con respecto a la forma en que un usuario de CS existente accede a una red de IMS.

La señalización de CS de interfaz de radio (por ejemplo, señalización GSM 04.08) se utiliza para registrar un usuario de CS móvil en el dominio de CS, pero la señalización de SIP, basada en una red de PS, se utiliza para registrar un usuario en el IMS. Por lo tanto, un usuario de CS es incapaz de registrarse para el IMS directamente. En la técnica anterior, por lo tanto, resulta imposible para un usuario de CS acceder a una red de IMS mediante su registro en dicha red de IMS.

Una solicitud de patente WO 00/33523 A da a conocer un sistema y un método para el registro de un terminal móvil en una red de conmutación de paquetes inalámbrica integrada, de modo que proporcione un sistema de registro dual para el terminal móvil utilizando una entidad compatible con H.323.

Una solicitud de patente US 2003/027595 A1 da a conocer una provisión de servicios, en un sistema de comunicaciones, que incluye un centro de conmutación móvil interfuncionamiento, para permitir una integración más fácil de los dominios de CS y de PS.

SUMARIO DE LA INVENCIÓN

Las formas de realización de la presente invención dan a conocer un sistema y un aparato para un usuario de CS móvil para acceder a una red de IMS y un método de registro para el acceso, lo que permite el registro de un usuario de CS móvil para la red de IMS de forma adecuada y el acceso a la red de IMS para obtener servicios ricos en contenidos.

Un sistema para un usuario de CS móvil para acceder a una red de IMS, dado a conocer en una forma de realización de la presente invención, comprende una red de IMS para proporcionar servicios de IMS y una red de acceso de CS y comprende, además:

una entidad de Función de Proxy de Registro (RPF) que incluye, además, una primera interfaz para comunicarse con la red de IMS y una segunda interfaz para comunicarse con la red de acceso de CS. La entidad de RPF está adaptada para poner en correspondencia un evento de registro de CS que tiene su origen en el usuario de CS móvil a través de la segunda interfaz con un evento de registro de IMS e iniciar el registro para la red de IMS a través de la primera interfaz en nombre del usuario de CS móvil;

en donde la iniciación del registro a la red de IMS, a través de la primera interfaz, en nombre del usuario de CS móvil, comprende:

el envío, por la entidad de RPF, del evento de registro de IMS mapeado, a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de realizar registros de IMS para el usuario de CS móvil, directamente, sin necesidad de la autenticación del usuario de CS móvil y concluir el proceso de registro, si la entidad de red de IMS determina que el registro se inicia por el usuario de CS móvil y el usuario de CS móvil está autenticado en el HLR de forma satisfactoria;

o,

el envío, por la entidad de RPF, del evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de la autenticación del usuario de CS de móvil y de realización del registro de IMS para el usuario de CS móvil, en función de la información transmitida en el evento de registro de IMS mapeado y la conclusión del proceso de registro, si la entidad de red de IMS determina que el registro se inicia por el usuario de CS móvil.

Un método de registro para permitir a un usuario de CS móvil tener acceso a una red de IMS dada a conocer en una forma de realización de la presente invención que comprende:

la puesta en correspondencia, o mapeado, por una entidad de RPF, de un evento de registro de CS con un evento de registro de IMS después de la detección de un evento de registro de CS iniciado por un usuario de CS móvil y

la iniciación, por la entidad de RPF, de un proceso de registro para la red de IMS a través del evento de registro de IMS;

en donde la iniciación del registro para la IMS, a través de la primera interfaz en nombre del usuario de CS móvil, comprende:

el envío, por la entidad de RPF, del evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de la autenticación del usuario de CS móvil y realizar el registro de IMS para el usuario de CS móvil, directamente, sin necesidad de la autenticación del usuario de CS móvil y concluir el proceso de registro, si la entidad de red de IMS determina que el registro se inicia por el usuario de CS móvil y el usuario de CS móvil es autenticado en el HLR de forma satisfactoria;

o,

el envío, por la entidad de RPF, del evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de realizar el registro de IMS para el usuario de CS móvil, en función de la información transmitida en el evento de registro de IMS mapeado y concluir el proceso de registro, si la entidad de red de IMS determina que el registro se inicia por el usuario de CS móvil.

Una entidad de RPF dada a conocer en una forma de realización de la presente invención comprende una primera interfaz para comunicarse con la red de IMS y una segunda interfaz para comunicarse con la red de acceso de CS y comprende, concretamente:

una unidad detectora de eventos de registros, adaptada para detectar un evento de registro de CS iniciado por un usuario de CS móvil a través de la segunda interfaz;

una unidad de mapeado, adaptada para mapear el evento de registro de CS detectado por la unidad detectora de eventos de registro para un evento de registro de IMS y

una unidad de registro de IMS, adaptada para registrar para la red IMS el nombre del usuario de CS móvil a través de la primera interfaz en función del resultado del mapeado de la unidad de mapeado;

en donde la iniciación del registro para la red de IMS, a través de la primera interfaz en nombre del usuario de CS móvil, comprende:

el envío, por la entidad de RPF, del evento de registro de IMS mapeado a una entidad de IMS, en donde la entidad de red de IMS es capaz de autenticar el usuario de CS móvil y realizar el registro de IMS para el usuario de CS móvil, directamente, sin necesidad de la autenticación del usuario de CS móvil y concluir el proceso de registro, si la entidad de red de IMS determina que el registro se inicia por el usuario de CS móvil y el usuario de CS móvil es autenticado en el HLR de forma satisfactoria;

o,

el envío, por la entidad de RPF, del evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de realizar el registro de IMS para el usuario de CS móvil, en función de la información transmitida en el evento de registro de IMS mapeado y concluir el proceso de registro, si la entidad de red de IMS determina que el registro se inicia por el usuario de CS móvil.

En la solución técnica anterior, dada a conocer por una forma de realización de la presente invención, una entidad de RPF se añade a la red, de modo que un usuario de CS móvil se pueda registrar para la red de IMS cuando se requiera permitiendo, de este modo, habilitar un usuario de CS para acceder a la red de IMS para disfrutar de servicios de IMS ricos en contenido.

Las formas de realización de la presente invención hacen viable, para un operador, unificar y simplificar la red de núcleo y reducir efectivamente el coste de la operación.

Las formas de realización de la presente invención permiten al dominio de CS móvil servir como una tecnología de acceso de la red de IMS y permitir a un usuario de CS móvil acceder a una red de IMS. El acceso integrado desde una red de CS a una red de IMS es de gran importancia con respecto a reducir los costes de explotación y efectuar el lanzamiento de servicios coherentes con rapidez.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama de flujo del registro de un usuario de CS móvil;

La Figura 2 representa la composición de una IMSI;

La Figura 3 representa la composición de un número MSISDN;

La Figura 4 es un diagrama de flujo del registro de un usuario de tarjeta SIM para un dominio de CS;

La Figura 5 representa la estructura de un sistema de IMS;

La Figura 6 ilustra la relación entre la identidad del usuario y los datos de servicios de un usuario de IMS;

La Figura 7 es un diagrama de flujo del registro inicial de un usuario de IMS;

La Figura 8 es un diagrama de flujo de re-registro de un usuario de IMS;

La Figura 9 es un diagrama de flujo de re-registro iniciado por una red de IMS;

La Figura 10 es un diagrama de flujo de de-registro iniciado por una red de IMS;

La Figura 11 ilustra la estructura de un sistema y aparato según una forma de realización de la invención;

La Figura 12 representa el proceso de una notificación de registro de capa de aplicación;

La Figura 13 es el primer diagrama de flujo del método según una forma de realización de la presente invención en el primer modo;

La Figura 14 es el segundo diagrama de flujo del método según una forma de realización de la presente invención en el primer modo;

La Figura 15 es el tercer diagrama de flujo del método según una forma de realización de la presente invención en el primer modo;

La Figura 16 es el cuarto diagrama de flujo del método según una forma de realización de la presente invención en el primer modo;

La Figura 17 es el quinto diagrama de flujo del método según una forma de realización de la presente invención en el primer modo;

La Figura 18 es el sexto diagrama de flujo del método según una forma de realización de la presente invención en el primer modo;

La Figura 19 es el primer diagrama de flujo del método según una forma de realización de la presente invención en el segundo modo;

La Figura 20 es el segundo diagrama de flujo del método según una forma de realización de la presente invención en el segundo modo,

La Figura 21 es el tercer diagrama de flujo del método según una forma de realización de la presente invención en el segundo modo;

La Figura 22 es el cuarto diagrama de flujo del método según una forma de realización de la presente invención en el segundo modo;

La Figura 23 es el quinto diagrama de flujo del método según una forma de realización de la presente invención en el segundo modo;

La Figura 24 es el sexto diagrama de flujo del método según una forma de realización de la presente invención en el segundo modo y

La Figura 25 es el séptimo diagrama de flujo del método según una forma de realización de la presente invención en el segundo modo.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN DE LA INVENCIÓN

Las formas de realización de la presente invención permiten el registro de un usuario de CS móvil, que necesita acceder a una red de IMS y concretamente, registrar un usuario de CS que se suscribe al servicio de IMS para la red de IMS. Las operaciones realizadas en el proceso de registro del usuario comprenden: la detección de un evento de registro; el mapeado del ID de dominio de un usuario de CS para un ID de dominio de IMS, el mapeado de la señalización de un proceso de registro de CS con la señalización de un proceso de registro de SIP, el mapeado de la parte adicional de un proceso de registro de IMS como contra el dominio de CS respecto al dominio de CS y la identificación de usuarios de CS registrados y operaciones especiales realizadas por cada entidad en la red de IMS. Las formas de realización de la presente invención dan a conocer un proceso de registro perfecto que permite a un usuario de CS móvil acceder a una red de IMS con miras a las operaciones anteriores que necesitan realizarse en el proceso de registro.

En primer lugar, las formas de realización de la presente invención dan a conocer un sistema para registrar un usuario de CS móvil que necesita acceder a una red de IMS. Según se representa en la Figura 11, una entidad de Función de Proxy de Registro (RPF) es añadida entre la red de CS y la red de IMS. A través de la entidad de RPF, el sistema se registra para la red de IMS en nombre del usuario de CS móvil, de modo que el usuario de CS móvil pueda acceder a la red de IMS. De esta forma, la red de IMS es compatible con un terminal de CS y un terminal de CS emulado por IMS. El “terminal de CS” y el “usuario de CS” anteriormente citados se refieren a un usuario de CS móvil. Para hacer más evidente la descripción, el usuario de CS móvil es referido como “UE” en adelante.

Las funciones de las entidades en el sistema dado a conocer en una forma de realización de la presente invención se describen a continuación con referencia a la Figura 11:

(i) RPF

Se añade un RPF en las formas de realización de la presente invención y se adapta para el registro para una red de IMS en nombre de un usuario de CS móvil, sobre la base de la herencia de las funciones relacionadas con el registro de un MSC y un VLR en el dominio de CS.

Para poner en práctica las formas de realización de la presente invención, un RPF comprende una primera interfaz para la comunicación con la red de IMS y una segunda interfaz para la comunicación con la red de CS. Las unidades de procesamiento básicas de un RPF comprenden:

(1) una unidad detectora de eventos de registro, adaptada para detectar el evento de registro de CS iniciado por un usuario de CS móvil a través de la segunda interfaz, a saber, un evento de registro de señalización de CS iniciado por un usuario de CS y la iniciación operativa de la unidad de mapeado, en donde un evento de registro puede ser un evento de registro o de de-registro;

(2) una unidad de mapeado, adaptada para efectuar el mapeado del evento de registro de CS con un evento de registro de IMS;

la unidad de mapeado comprende, además, una unidad de mapeado de identidades, adaptada para poner en correspondencia el ID de dominio de CS de un usuario de CS móvil con un ID de dominio de IMS, según un modo de mapeado predeterminado;

(3) una unidad de registro de IMS, adaptada para el registro para la red de IMS en nombre de un usuario de CS a través de la primera interfaz, en función del evento de registro de IMS mapeado por la unidad de mapeado, es decir, la unidad

de registro de IMS está adaptada para el registro para el dominio de IMS en nombre de un usuario de CS móvil. En el proceso de registro, la unidad de mapeado necesita exportar la identidad del usuario en el dominio de CS móvil para la identidad de usuario y el identificador ID de red base requerido para el registro en el dominio de IMS.

Además de las unidades de procesamiento básicas anteriores, al menos una de estas unidades de procesamiento adicionales deben existir en un RPF: una unidad de autenticación de IMS, una unidad de suscripción de eventos de registro de usuarios, una unidad de iniciación de re-registro, una unidad de de-registro del usuario y una unidad de suscripción de eventos de transferencias de usuarios.

Las unidades de procesamiento adicionales anteriores están adaptadas para poner en práctica las funciones siguientes:

realización de la autenticación en el dominio de IMS en nombre de un usuario de CS móvil;

la suscripción a los eventos de registro de usuarios, con la notificación de un usuario de CS móvil para iniciar el re-registro;

la operación de re-registro para una red de IMS en nombre de un usuario de CS móvil;

la operación de de-registro desde la red de IMS en nombre de un usuario de CS móvil;

la notificación a una red de usuario de CS móvil para iniciar el de-registro y

la habilitación de otras entidades de red de IMS para suscribir los eventos de transferencias de un usuario de CS móvil registrado.

Además, un RPF puede comprender también una unidad de registro de CS, adaptada para registrar un usuario de CS para un dominio de CS a través de una tercera interfaz entre el RPF y la base de datos de suscripción de CS (por ejemplo, un HLR o un HSS que almacena información de dominios de CS). Como alternativa, el RPF, en una forma de realización de la presente invención, se puede establecer sobre una entidad (por ejemplo, MSC/VLR), que está situada en el dominio de CS y adaptada para poner en práctica la función de registro (cuando se establece un RPF en un MSC/VLR, pudiéndose reducir o aumentar las funciones de MSC/VLR). Las funciones del RPF se realizan a través de la interfaz proporcionada para la comunicación con la red de IMS.

(ii) Servidor de Abonados Base (HSS).

El HSS es un servidor de abonados de IMS base que existe ya en la red de IMS. Está adaptado para gestionar datos de usuarios y generar datos de autenticación para usuarios de CS. Un usuario de CS puede ser objeto de autenticación, en el dominio de IMS directamente, si el HSS contiene los datos de autenticación del usuario de CS.

(iii) HLR

El HLR es un servidor de abonados de CS base en una red de IMS. Como una entidad existente en la red de CS, el HLR está adaptado para almacenar datos de suscripción de usuarios de CS. Los datos de suscripción se pueden utilizar para la autenticación de usuarios de CS.

Las funciones del HLR son funciones opcionales del sistema, dadas a conocer por una forma de realización de la presente invención. El HLR es requerido, en una forma de realización de la presente invención, solamente en un modo de registro específico, esto es, solamente cuando la autenticación para el UE es inviable en el dominio de IMS y debe realizarse en el dominio de CS. A través del HLR, se pone en práctica la autenticación del usuario de CS.

En un proceso de aplicación específico, el HLR y el HSS, representados en la figura, se pueden combinar en un HSS o funcionar de modo independiente.

(iv) Función de Control de Sesión de Llamadas (CSCF)

La CSCF es una entidad de la red de IMS. En particular, la CSCF-Servidor (S-CSCF) identifica un usuario como un usuario de CS, que accede a la red de IMS, y funciona con el HSS para la autenticación del usuario de CS móvil en la red de IMS. No obstante, si no se requiere ninguna autenticación para el usuario en el dominio de IMS, dicho procesamiento es innecesario.

En el sistema dado a conocer por la presente invención, una Red de Acceso de Radio (RAN) puede ser, pero no está limitada a ser: una red UTRAN o GERAN definida por el protocolo 3GPP o una red RAN definida por 3GPP2.

En la Figura 11, dependiendo de la posición del RPF, si el RPF y el P-CSCF funcionan en la misma entidad, la interfaz A es una interfaz de Mw definida por el IMS; de no ser así, la interfaz A es una interfaz de Gm definida por el IMS. La interfaz B es una interfaz conectada al HSS del usuario cuando el RPF pone en práctica el registro de un usuario de CS

móvil mediante la señalización de CS. En la aplicación, la interfaz B puede ser, pero no está limitada a ser: una interfaz definida por el protocolo 3GPP o una interfaz de MAP definida por el 3GPP2. La interfaz B es opcional en las formas de realización de la presente invención. La interfaz C es una interfaz entre la RPF y la RAN. En la aplicación, la interfaz C puede ser, sin limitación: interfaz Iu o interfaz A definida por el protocolo 3GPP o una interfaz A definida por el protocolo 3GPP2.

El método para habilitar un usuario de CS móvil para acceder a la red de IMS, dada a conocer en una forma de realización de la presente invención, se describe a continuación.

En el método según la presente invención, ante todo, una entidad de RPF necesita detectar eventos relacionados con el registro, a saber, detectar los eventos de registro iniciados por usuarios de red no de IMS; más adelante, la entidad de RPF inicia el registro para la red de IMS en nombre del usuario de CS móvil.

Según se ilustra en la Figura 11, cuando el RPF inicia el registro para la red de IMS en nombre de un usuario de CS móvil, el proceso de registro se puede realizar en los dos modos siguientes, dependiendo del tiempo de registro y del modo de autenticación:

Modo 1: Registro del usuario en el HLR mediante la interfaz B y, si fuera satisfactorio, registro del usuario en el HSS a través de la interfaz A.

El proceso de registro detallado, en el primer modo, es como sigue:

(1) El RPF se registra para el dominio de CS en el HLR, en nombre del usuario a través de la interfaz B. El proceso de registro específico se pone en práctica por la entidad de función básica en el RPF. Puesto que el usuario es un usuario de CS, el proceso de registro es el mismo que el de la técnica anterior.

(2) El RPF registra el usuario para IMS a través de la interfaz A, después de registrar al usuario para el dominio de CS de forma satisfactoria.

La etapa (2) comprende, además:

(2-1) El RPF pone en correspondencia y convierte un evento de registro CS, o parámetro, con respecto a un evento de registro de IMS o parámetro. El proceso de puesta en correspondencia y de conversión comprende:

(2-1-1) El RPF pone en correspondencia un ID de dominio de CS del usuario con un ID de dominio de IMS.

Es decir, el RPF necesita convertir el ID de dominio de CS del usuario en un ID de dominio de IMS cuando se registra para la red de IMS en nombre del usuario de CS, incluyendo los procesos de convertir uno o más de los identificadores IDs siguientes en el identificador ID de dominio de IMS correspondiente:

(2-1-1-1) Se genera un nombre de dominio base.

Más concretamente, se pueden utilizar cinco o seis dígitos en la IMSI, dependiendo de la longitud del MNC. El identificador ID del protocolo 3GPP se añade al MNC y al MCC para generar un nombre de dominio base. En general, el formato de un nombre de dominio base generado es: ims.mnc<real MNC>.mcc<MCC>.3gppnetwork.org; por ejemplo, si una IMSI es 234150755999999, MCC = 234 y MNC = 15, en cuyo caso el nombre de dominio base generado es: ims.mnc15.mcc234.3gppnetwork.org.

Además, un número de subdominio (SDN, que consiste en varios dígitos después del MNC en la IMSI) se puede añadir sobre la base del método de 3GPP anterior. El identificador ID del 3GPP se añade para generar un nombre de dominio base. En general, el formato de un nombre de dominio base generado es: ims. mnc<real MNC>.mcc<MCC>.sdn<SDN>3gppnetwork.org; por ejemplo, si una IMSI es 234150755999999, MCC = 234 y MNC = 15 y el SDN del operador en una zona determinada es 0755, en cuyo caso el nombre de dominio base generado es: ims.mnc15.mcc234.sdn0755.3gppnetwork.org.

(2-1-1-2) Se generan IMPU e IMPI temporales.

De forma similar, las IMPU e IMPI temporales se pueden generar en función de la IMSI del usuario, el formato de una IMPU temporal es “SIP: identidad usuario@nombre dominio base” y el formato de una IMPI es “identidad usuario @nombre dominio base”, en donde la identidad del usuario se genera en función de la IMSI del usuario de CS directamente y el nombre de dominio base se genera en el método anterior. Por ejemplo, si una IMSI es 234150755999999, las IMPU e IMPI temporales pueden ser:

SIP: 234150755999999@ ims.mnc15.mcc234.sdn0755.3gppnetwork.org

y 234150755999999@ ims.mnc15.mcc234.sdn0755.3gppnetwork.org

(2-1-1-3) Una vez registrado el usuario de CS para la red de IMS, la IMPU por defecto reenviada se genera en el formato de “E.164 número @ nombre dominio base” y se memoria en el HSS, S-CSCF, RPF o AS, de modo que sirva como una IMPU por defecto del usuario en la red de IMS.

Suponiendo que una IMPU es 8613907551234@sz.gd.cmcc.com, el usuario utiliza esta IMPU a través de toda la red de IMS y el número de E.164 del usuario se puede exportar en función de la IMPU del usuario. En la red de IMS base del usuario, la IMPU del usuario se puede exportar también en función del número E.164 del usuario o la IMPU del usuario puede encontrarse a través del servicio de ENUM en función del número E.164 del usuario.

(2-1-2) El RPF pone en correspondencia el evento de registro de CS detectado con un evento de registro de IMS e inicia el registro para la red de IMS.

Más concretamente, el RPF establece la correspondencia del evento de registro de CS detectado. El proceso de mapeado específico es como sigue:

“UE power-on” es objeto de mapeado para “registro inicial IMS”;

“Actualización de posición inicial después de la itinerancia a una nueva zona de posición” se mapea con “registro inicial de IMS” y

la “Actualización de posición periódica” se pone en correspondencia con “re-registro de IMS”.

(22) La red de IMS realiza la autenticación del usuario de CS. El proceso de autenticación comprende:

Cuando se gestiona una petición de Registro, si la S-CSCF identifica que el solicitador de registro es un usuario de CS, la S-CSCF decide poner en práctica el registro directamente sin iniciar un proceso de autenticación para el usuario.

El proceso específico de identificación de un usuario de CS registrado en una red de IMS es como sigue:

Un usuario de CS se identifica en función de la identidad del usuario en la petición; la S-CSCF y el HSS pueden resolver la identidad del usuario en función de la configuración de la red y a continuación, juzgar si el usuario de CS está registrado, o no, en función de la identidad de usuario resuelta. La identidad de usuario puede ser, sin limitación: una IMPU o IMPI temporal utilizada en el registro.

El proceso de identificación se puede realizar, además, en función del parámetro específico o una combinación de diferentes valores de parámetros en la petición de Registro. La información detallada sustentada en el parámetro o combinación de parámetros se decide por la gestión del Elemento de Red (NE). Por ejemplo, en una S-CSCF, el proceso de identificación se realiza en función del parámetro en la petición de Registro recibida incluyendo, sin limitación, el parámetro del campo de cabecera de Autorización tal como “auth-scheme”; en el HSS, el proceso de identificación se realiza en función del parámetro en la petición de autenticación recibida incluyendo, sin limitación, el parámetro de “auth-scheme”, que indica el sistema de autenticación soportado por un terminal y en términos más amplios, el parámetro que indica los atributos de la red de acceso.

(23) El usuario de CS se registra en el dominio de IMS. En el HSS y cada CSCF, necesita actualizarse la información de registro del usuario y de forma opcional, se suscribe al evento de registro del usuario. La actualización de información de registro del usuario comprende: marcado del usuario de CS como registrado y así sucesivamente.

El proceso de registro comprende, además:

Cuando el HSS recibe una petición de datos de usuarios de la S-CSCF en el proceso de registro, el HSS identifica el usuario de CS en función de la identidad del usuario en la petición y verifica el resultado de autenticación previo del usuario en el HLR. Si la autenticación en el HLR tiene éxito, el HSS continúa con el registro de IMS; en caso contrario, el HSS rechaza el registro en el dominio de IMS.

Como alternativa, el HSS puede registrar el usuario para el dominio de IMS directamente sin necesidad de autenticación del usuario en el HLR.

Modo 2: El RPF registra el usuario en el HSS en el IMS solamente a través de la interfaz A.

El proceso de registro detallado, en el segundo modo, es como sigue:

(1) El RPF efectúa el mapeado y convierte un evento de registro de CS, o parámetro, en un evento de registro de IMS o parámetro. El proceso de mapeado y conversión comprende:

El RPF realiza el mapeado del ID de dominio de CS del usuario con un ID de dominio de IMS. Para el proceso detallado, ver la contrapartida del primer modo.

El RPF efectúa el mapeado del evento de registro de CS detectado con un evento de registro de IMS. Para el proceso detallado ver la contrapartida del primer modo.

El RPF efectúa el mapeado de la capacidad de autenticación soportada por el terminal de CS detectado para el parámetro en el mensaje de registro de SIP e inicia el registro para la red de IMS. El mapeado de la capacidad de autenticación del terminal se puede realizar en uno de estos modos: modo GSM, modo UMTS y modo CDMA. Más concretamente, el parámetro en el campo de cabecera de Autorización, en el mensaje de Registro de SIP, se puede extender para transmitir la información de capacidad de autenticación, por ejemplo, parámetro extendido “auth-scheme”. De este modo, la capacidad de autenticación del terminal anterior es mapeada con “GSM-AKA”, “UMTS-AKA” y “CDMA-AKA”, respectivamente.

(2) La red de IMS realiza la autenticación del usuario de CS. Dicho proceso de autenticación comprende:

En primer lugar, la S-CSCF recibe una petición de Registro inicial. Después de determinar que la petición es una petición de Registro del usuario de CS, la S-CSCF solicita al servidor HSS información de autenticación en función de los parámetros en la petición y especifica el sistema de autenticación soportado por el usuario y otra información relacionada con la autenticación. El proceso detallado de la identificación de una petición de Registro del usuario de CS se describió anteriormente y no se repite a continuación.

En este caso, el proceso detallado de determinación del sistema de autenticación y otra información relacionada con la autenticación es: la S-CSCF determina el sistema de autenticación de la petición enviada al HSS en función del parámetro extendido del campo de cabecera de Autorización, por ejemplo, “auth-scheme” y exporta el tipo de la red de acceso en función del campo de cabecera de “P-acceso-Red-Info”. De este modo, se obtienen los dos parámetros que necesitan incluirse en el mensaje de petición de autenticación enviado al HSS.

Más adelante, después de recibir la petición de autenticación enviada desde la S-CSCF, el HSS genera vectores de autenticación (AVs) adecuados en función de la información contenida en el mensaje de petición. Después de procesar dichos vectores AVs, el servidor HSS reenvía los vectores AVs a la S-CSCF, que realizará la autenticación del usuario.

Concretamente, el HSS determina el tipo de AV en uso en función de los atributos del usuario y juzga si realizar, o no, la conversión entre un vector quintupleto y un vector tripleto en función del tipo de red de acceso que se recibe, el sistema de autenticación soportado por el UE y la información de atributo del usuario; en adelante, el HSS reenvía el AV final a la S-CSCF y especifica el sistema de autenticación puesto en práctica en la red.

(3) El usuario de CS se registra para el dominio de IMS y al usuario se le notifica la conclusión del registro.

El proceso detallado se describe a continuación.

En primer lugar, los elementos NEs pertinentes en el dominio de IMS actualizan el estado de registro del usuario, esto es, actualizan el usuario de CS como un usuario registrado y, de forma opcional, realizan un procesamiento posterior tal como una suscripción a eventos de registro del usuario.

Más adelante, el RPF efectúa el mapeado de la red 200 OK, que se recibe cuando el RPF se registra al dominio de IMS en nombre del usuario, para un mensaje de “aceptación de actualización de posición” del dominio de CS, indicando que el registro está concluido.

Otros procesos posibles posteriores al registro del usuario de CS para el dominio de IMS comprenden: re-registro, suscripción y de-registro. Los procesos de mapeado de re-registro, de-registro y suscripción son mutuamente independientes.

Los posibles procesos posteriores al registro se describen a continuación.

(1) El RPF inicia la suscripción a eventos de registro de usuarios en nombre de usuario de CS móvil.

Después de detectar la conclusión del registro para el dominio de IMS, el RPF inicia la suscripción a eventos de registro de usuarios en nombre del usuario. Si el RPF está situado en la P-CSCF, el RPF necesita también iniciar la misma suscripción en nombre de la P-CSCF.

(2) El RPF se de-registra desde la red de IMS en nombre del usuario de CS móvil.

Si el RPF detecta un evento de desconexión del usuario de CS móvil o un mensaje de cancelar posición, el RPF inicia el de-registro en nombre del usuario.

(3) El RPF gestiona el proceso de de-registro del usuario iniciado por la red de IMS.

Después de recibir el mensaje de de-registro del usuario desde la red, el RPF utiliza la señalización o aplicación relacionada con CS para notificar al usuario que está de-registrado desde el dominio de IMS.

Según se representa en la Figura 12, para redes de GSM y WCDMA, si la interfaz de radio no tiene ningún proceso de señalización adecuado cuando la red inicia el de-registro, se pueden aplicar las prácticas en la capa de aplicación, por ejemplo, utilizando un mensaje corto, Datos de Servicios Suplementarios No Estructurados (USSD) o anuncio de la red para notificar al usuario que está de-registrado desde el dominio de IMS, de modo que el usuario conozca su estado a tiempo.

(4) El RPF gestiona el re-registro del usuario iniciado por la red de IMS.

En el primer modo anteriormente descrito, el RPF puede iniciar un re-registro para la red de IMS en nombre del usuario después de recibir una petición de re-registro del usuario desde la red.

En el segundo modo anteriormente descrito, el RPF utiliza la señalización relacionada con CS, o su aplicación, para notificar al usuario que se inicia un proceso de registro después de recibir una petición para re-registro del usuario desde la red.

Según se representa en la Figura 12, para redes GSM y WCDMA, cuando la red inicia el re-registro, si la interfaz de radio no tiene un proceso de señalización adecuado, se puede aplicar la práctica en la capa de aplicación, por ejemplo, utilizando un mensaje corto, USSD o un anuncio de red en la técnica anterior para notificar al usuario y poner en práctica el proceso de re-registro; si se notifica al usuario a través de un mensaje corto o USSD y el UE es capaz de gestionar el proceso, el UE inicia el re-registro automáticamente después de la notificación al usuario; si el usuario es incapaz de gestionar, se necesita visualizar una notificación de re-registro al usuario y el usuario decidirá si iniciar, o no, el registro de nuevo; si se notifica al usuario a través de un anuncio de red, le corresponde al usuario decidir si iniciar, o no, un registro de nuevo.

(5) El RPF gestiona la suscripción a eventos de transferencia de usuarios iniciados por otras entidades de red de IMS y la notificación de eventos correspondiente.

Después de que el RPF termine el registro para el dominio de IMS en nombre de un usuario de CS, el RPF solicita a las entidades de red interesadas en el evento de transferencia de usuarios suscribirse al evento de transferencia al RPF. Es decir, una entidad en la red de IMS puede suscribirse al evento de transferencia de usuarios susceptible de percepción en el RPF, incluyendo la transferencia en el interior de RPF y la transferencia entre RPFs.

Después de gestionar la petición, el RPF notifica el evento de transferencia de usuario detectado a las entidades que han suscrito los eventos de transferencia. Es decir, después de detectar la conclusión de la transferencia, el RPF notifica el evento correspondiente al abonado.

(6) La entidad de RPF se re-registra a la red de IMS en nombre del usuario de CS.

Después de recibir una petición de re-registro desde el usuario, el RPF puede iniciar el re-registro para la red de IMS en nombre del usuario de CS móvil.

Para hacer más evidente la solución técnica dada a conocer en la presente invención, se describe, a continuación, en detalle, haciendo referencia a las formas de realización y a los dibujos adjuntos.

Forma de realización 1

En la primera forma de realización, el proceso de registro inicial realizado en el modo 1, antes de que un usuario de CS móvil pueda acceder a una red de IMS, se describe a continuación. Aunque la tecnología de WCDMA se utiliza como un ejemplo en esta descripción, la aplicación de la presente invención no está limitada a la tecnología de WCDMA. El RPF está combinado con la P-CSCF en la forma de realización, pero no está previsto para limitar la aplicación real de la presente invención.

Según se representa en la Figura 13, la primera forma de realización comprende las etapas siguientes:

Etapa 131: Después de concluir el registro desde el dominio de CS para el HLR en nombre del usuario, el RPF realiza el mapeado del ID de dominio de CS con el ID de dominio de IMS, elabora un mensaje de Registro de la red de IMS y lo envía a la red de IMS.

La conversión detallada desde un ID de dominio de CS a un ID de dominio de IMS se describió anteriormente y no se repetirá a continuación.

Etapa 132: Cuando se gestiona una petición de Registro, si la S-CSCF identifica que el solicitador de registro es un usuario de CS, la S-CSCF decide notificar al HSS el éxito del registro del usuario, directamente, sin iniciar un proceso de autenticación para el usuario porque el usuario de CS ha pasado la autenticación y registro en el HLR.

En la etapa 132, el proceso detallado de la S-CSCF que identifica si el usuario es un usuario de CS, o no, se describió anteriormente y no volverá a repetirse.

Etapa 133: El HSS y las CSCFs actualizan la información de registro del usuario. Hasta ahora, el usuario de CS ha sido registrado en el dominio de IMS con éxito.

En la etapa 133, la actualización de información de registro del usuario comprende: el marcado del usuario de CS como registrado.

Forma de realización 2

En el primer modo, el proceso de registro inicial antes de que un usuario de CS móvil pueda acceder a una red de IMS se representa en la Figura 14. Aunque el sistema de WCDMA se utiliza como un ejemplo en esta forma de realización, la aplicación de la presente invención no está limitada al sistema de WCDMA. La Figura 14 supone que el RPF está combinado con la P-CSCF, pero ello no está previsto para limitar la aplicación real de la presente invención.

En la Figura 14, en el proceso de registro inicial en el primer modo, el proceso para un HSS para verificar el resultado de autenticación de HLR comprende:

Etapa 141: Después de concluir el registro desde el dominio de CS al HLR en nombre del usuario, el RPF pone en correspondencia el ID del dominio de CS del usuario de CS con el ID del dominio de IMS, elabora un mensaje de Registro de la red de IMS y lo envía a la red de IMS.

Etapa 142: Cuando se gestiona la petición de Registro, si la S-CSCF identifica que el solicitador del registro es un usuario de CS, la S-CSCF decide notificar al HSS el éxito del registro del usuario directamente sin iniciar un proceso de autenticación para el usuario y solicita los datos del usuario.

Etapa 143: El HSS consulta el HLR para conocer el resultado de autenticación del usuario a través de una interfaz con el HLR.

Etapa 144: El HLR consulta el estado del usuario en función de la identidad del usuario proporcionada por el HSS y reenvía el resultado de la consulta al HSS.

Etapa 145: El HSS y las entidades CSCFs actualizan la información de registro del usuario. Hasta aquí, el usuario de CS ha sido registrado para el dominio de IMS con éxito.

Forma de realización 3

En el primer modo, cuando un usuario de CS móvil desconecta el UE, el RPF efectúa el mapeado del evento de “desconexión del usuario” para el “de-registro de IMS iniciado por el usuario”. El proceso de de-registro se representa en la Figura 15, en el supuesto de que el RPF está combinado con la P-CSCF;

En la Figura 15, en el primer modo, el proceso de de-registro iniciado por el usuario comprende:

Etapa 151: Cuando se detecta un evento de desconexión de un usuario de CS, el RPF puede iniciar un de-registro para la red de IMS en nombre del usuario después de establecer el estado del dominio de CS. Los parámetros son los mismos que los existentes en el registro inicial, con la excepción de que el campo “expira” después del campo “Contacto” se pone a 0, lo que significa que el usuario necesita un de-registro. En función del nombre de dominio base del usuario, el RPF resuelve la dirección de la I-CSCF base. En adelante, el RPF envía un mensaje de Registro de SIP.

Etapa 152: En función de la IMPU y de la IMPI del usuario, la I-CSCF consulta el HSS para conocer el estado de registro del usuario. Si el usuario es legal y está registrado, el HSS reenvía a la S-CSCF la información de la dirección y la I-CSCF reenvía la petición de Registro a la dirección de S-CSCF reenviada o seleccionada.

Etapa 153: Puesto que el valor del campo “expira” de la petición es 0, la S-CSCF conoce que el usuario necesita un de-registro. Por lo tanto, la S-CSCF notifica al HSS la actualización del estado de registro del usuario y reenvía un mensaje 200 OK al RPF.

Etapa 154: Después de recibir el mensaje 200 OK, el RPF borra la información relacionada con el usuario, memorizada en el RPF, con lo que se concluye el proceso de de-registro en el caso de desconexión del usuario.

Forma de realización 4

En el primer modo, cuando un usuario de CS móvil accede a una red de IMS, la red de IMS inicia un proceso de de-registro. El proceso de de-registro se representa en la Figura 16, en donde el HSS decide el de-registro del usuario, suponiendo que el RPF está combinado con la P-CSCF. Debe hacerse constar que el proceso de de-registro es también aplicable al segundo modo.

Según se representa en la Figura 16, el proceso de de-registro comprende las etapas siguientes:

Etapa 171: El HSS notifica a la S-CSCF para el de-registro del usuario.

Etapa 172: La S-CSCF envía un mensaje NOTIFY al usuario y la P-CSCF en función de la información de registro y suscripción del usuario y la P-CSCF, que indica que el usuario está en condición de de-registro y establece el atributo de eventos del campo “Contacto” del mensaje a “rechazado”; después de recibir el mensaje, el RPF notifica al UE que el UE está de-registrado desde el IMS a través de la capa de aplicación. En este caso, el UE ya no será capaz de iniciar un servicio de IMS.

Etapa 173: Después de recibir todos los mensajes 200 OK reenviados, la S-CSCF notifica al HSS la conclusión del de-registro.

Forma de realización 5

En el primer modo, el proceso de re-registro, iniciado por la red cuando un usuario de CS móvil accede a la red de IMS, se representa en la Figura 17, en donde la S-CSCF notifica al usuario la iniciación del re-registro después del intervalo de espera de registro, suponiendo que el RPF está combinado con la función P-CSCF. Conviene señalar que el proceso de re-registro es también aplicable al segundo modo.

En la Figura 17, en el primer modo y en el segundo modo, el proceso de re-registro, iniciado por la red, comprende las etapas siguientes:

Etapa 181: Después de detectar la terminación de la duración del registro del usuario, la S-CSCF notifica al usuario el re-registro.

En función de la información de registro y de suscripción del usuario y la entidad P-CSCF, la S-CSCF envía un mensaje NOTIFY al usuario y a la entidad P-CSCF, notificando al usuario la iniciación del re-registro y establece el atributo del evento del campo de “Contacto” del mensaje a “desactivado”;

Etapa 182: Después de recibir la notificación de re-registro desde la S-CSCF, el RPF notifica al UE la iniciación del re-registro a través de la capa de aplicación.

Etapa 183: El UE inicia el re-registro.

Etapa 184: Después de recibir todos los mensajes 200 OK reenviados por el RPF en nombre del usuario y reenviados por la P-CSCF, la S-CSCF notifica al HSS el estado del usuario.

Forma de realización 6

En el primer modo, el proceso para una red de suscripción a los eventos de transferencias de usuarios cuando un usuario de CS móvil accede a una red de IMS, se representa en la Figura 18, en el supuesto de que el RPF está combinado con la entidad P-CSCF. Conviene señalar que este proceso es también aplicable al segundo modo.

La Figura 18, en el primer modo y en el segundo modo, el proceso para una red para la suscripción a eventos de transferencia de usuarios comprende las etapas siguientes:

Etapa 191: Después del éxito del registro del usuario, la S-CSCF inicia un proceso de suscripción a eventos de transferencias al usuario.

Etapa 192: Cuando se requiere, el servidor de aplicación (AS) puede iniciar el proceso de suscripción de los eventos de transferencias al usuario, después de que el usuario se registre con éxito. El servidor AS percibe el registro a través del registro de un tercero.

Etapa 193: El UE inicia un proceso de transferencia. A la conclusión de la transferencia, el UE notifica al abonado que ocurre un evento de transferencia mediante un mensaje de notificación. El mensaje transmite el ID de la nueva zona de posición o el ID de celda y otros parámetros que son de interés para el abonado. Dependiendo del tipo de transferencia tal como una transferencia intraoficina, transferencia inter-oficinas y transferencia posterior, el abonado puede especificar uno o más tipos de los eventos de transferencias que han de suscribirse en el proceso de suscripción.

Las siete formas de realización anteriores describen la puesta en práctica de la presente invención en el primer modo. Las siguientes formas de realización describen, además, la puesta en práctica de la presente invención en el segundo modo.

Forma de realización 7

En el segundo modo, el proceso de registro inicial realizado antes de que un usuario de CS móvil pueda acceder a una red de IMS, se representa en la Figura 19. Aunque el subsistema de red de radio (RNS) del sistema de WCDMA se utiliza aquí como ejemplo, la aplicación de la presente invención no está limitada al sistema de WCDMA.

Según se representa en la Figura 19, el proceso de registro inicial detallado comprende las etapas siguientes:

Etapa 201: El RPF envía un mensaje de Registro a la entidad I-CSCF.

Los detalles de esta etapa son.

En primer lugar, después de detectar la “petición de actualización de posición” enviada por el UE, el RPF exporta el identificador ID requerido para el registro de IMS, en varios modos anteriormente descritos, en función del ID de dominio de CS del usuario de CS.

Más adelante, en función del nombre del dominio base exportado, el RPF resuelve la dirección de la I-CSCF base y envía un mensaje de Registro de SIP a la I-CSCF de la red de IMS, en cuanto al registro del usuario de CS para la red de IMS.

El mensaje de Registro comprende un parámetro extendido del campo de cabecera de Autorización, por ejemplo, “auth-scheme”. El parámetro extendido está adaptado para indicar el sistema de autenticación que se soporta por el UE y derivado de la señalización de CS recibida desde el Subsistema de Red de Radio (RNS); además, el mensaje de Registro incluye información de red de acceso en el campo de cabecera “P-acceso-red-info”. En este caso, la red de acceso puede estar en el modo de Red de Acceso de Radio Terrestre Universal – Dúplex por División de Frecuencia (UTRAN – FDD).

Etapa 202: La entidad I-CSCF reenvía el mensaje de petición de Registro a la S-CSCF seleccionada o determinada.

En función de la IMPU y de la IMPI del usuario, la I-CSCF consulta al HSS en cuanto al estado de registro del usuario. Si el HSS determina que el usuario es legal y no registrado, el HSS reenvía la información de capacidad de S-CSCF. En función de la información de capacidad, la I-CSCF selecciona una S-CSCF para gestionar la petición de Registro. Más adelante, la I-CSCF reenvía el mensaje de petición de Registro a la dirección de S-CSCF seleccionada. Si el HSS determina que el usuario es legal y registrado, el HSS reenvía la información de dirección de S-CSCF. Más adelante, la I-CSCF reenvía el mensaje de petición de Registro a la dirección de S-CSCF reenviada.

Etapa 203: Después de recibir el mensaje de petición de Registro, la S-CSCF comprueba la identidad del usuario en el mensaje y determina que el solicitador de registro es un usuario que accede a la red desde el dominio de CS y envía un mensaje de petición de autenticación multimedia al HSS. Este mensaje indica el sistema de autenticación soportado por el UE y el tipo de la red de acceso, de modo que el HSS pueda obtener los datos de autenticación correspondientes.

Etapa 204: Después de recibir la petición de autenticación multimedia, el HSS determina que el usuario es un usuario de CS USIM en función de la identidad del usuario. Por lo tanto, el HSS genera un vector de autenticación de quintupleto correspondiente (AV) para el usuario, indica que el sistema de autenticación puesto en práctica por la red es el acuerdo de claves de autenticación de la conmutación de circuitos del sistema universal de telecomunicaciones móviles (AKA-UMTS-CS) y luego reenvía el resultado a la S-CSCF.

Etapa 205: Después de recibir una respuesta de autenticación que soporta la información de resultado desde el HSS, la S-CSCF elimina el parámetro “XRES” (respuesta prevista) en el vector de autenticación (AV) y guarda la respuesta de autenticación. Más adelante, la S-CSCF inicia un desafío de autenticación al usuario reenviando un mensaje 401 al RPF a través de I-CSCF y establece el parámetro de “algoritmo” en el campo de cabecera de “WWW-Autenticar” para “AKA-UMTS-CS” que es un sistema de autenticación de red indicado por el servidor HSS.

Etapa 206: Después de recibir el mensaje de desafío de autenticación 401, el RPF genera un mensaje de petición de autenticación de dominio CS correspondiente y lo envía al UE a través del RNS.

Etapa 207: Después de recibir la petición de autenticación, el UE calcula el resultado de la autenticación en función del parámetro de autenticación recibido y lo reenvía al RPF a través del RNS. El RPF envía un segundo mensaje de petición de Registro a la S-CSCF a través de la I-CSCF.

Si la configuración de la red requiere un proceso de seguridad de dominio de CS, el RPF puede iniciar un segundo registro para la red de IMS, después de recibir un mensaje de "conclusión de protección de seguridad".

Si el dominio de CS no requiere ningún proceso de seguridad, el RPF puede iniciar un segundo registro para la red de IMS después de recibir la "respuesta de autenticación" del UE desde el RNS.

Etapa 208: Después de recibir la segunda petición de Registro reenviada por la I-CSCF, la S-CSCF compara la RES (respuesta de autenticación) enviada desde el UE con la XRES (exceptuada respuesta) almacenada en la S-CSCF; si coinciden, la autenticación ha sido un éxito y en caso contrario, falla la autenticación.

Después de los éxitos de la autenticación, la S-CSCF notifica al HSS del éxito del registro del usuario, descarga datos del usuario desde el HSS y a continuación, reenvía un mensaje 200 OK al RPF; la S-CSCF puede iniciar un registro de terceros para el AS, dependiendo de la inspección realizada como contra la condición de filtrado inicial (iFC).

Etapa 209: Después de recibir el mensaje 200 OK, el RPF actualiza el estado del usuario almacenado, la información de direcciones y el valor del intervalo de espera del registro y reenvía un mensaje de "aceptación de la actualización de posición" al UE, con la TMSI recientemente asignada transmitida en el mensaje; más adelante, el RPF envía un mensaje de petición a la S-CSCF para suscribirse a la notificación del estado de registro del usuario; después de recibir la petición de suscripción, la S-CSCF responde con un mensaje NOTIFY que transmite la información de registro del usuario, incluyendo todas las IMPUs registradas, que no estén prohibidas.

Etapa 210: Después de concluir el registro de terceros en la S-CSCF, el servidor AS recupera los datos de usuario pertinentes desde el HSS y se suscribe a los eventos de cambios de datos de usuarios.

Forma de realización 8

En el segundo modo, el proceso de registro inicial, realizado antes de que un usuario de CS móvil pueda acceder a una red de IMS, se representa en la Figura 20. Es decir, el proceso para una tarjeta USIM de un terminal 3G para acceder a la red a través del subsistema de estación base de GSM (BSS) incluye las etapas siguientes:

Etapa 211: Después de detectar la petición de actualización de posición enviada por el UE, el RPF exporta el ID requerido para el registro al dominio de IMS, en función del ID de dominio de CS del usuario de CS y resuelve la dirección de la I-CSCF de base, en función del nombre del dominio base exportado; más adelante, el RPF envía un mensaje de Registro de SIP a la I-CSCF para el registro de la red IMS; el mensaje de Registro debe transmitir el parámetro extendido del campo de cabecera de "Autorización", por ejemplo "auth-scheme", para indicar el sistema de autenticación que se soporta por el UE y obtenido por el RPF en función de la señalización de CS recibida desde el RNC; el mensaje de Registro soporta también la información de red de acceso en el campo de cabecera de "P-acceso-red-info". En esta forma de realización, la red de acceso está en un modo de Red de Acceso de Radio Mejorada de GSM (GERAN).

Etapa 212: En función de la IMPU y de la IMPI del usuario, la I-CSCF consulta al HSS para conocer el estado de registro del usuario. Si el HSS determina que el usuario es legal y no está registrado, el HSS reenvía la información de capacidad de S-CSCF y la I-CSCF selecciona una S-CSCF para gestionar la petición de Registro del usuario. Si el usuario es legal y está registrado, el HSS reenvía la información de dirección de la S-CSCF y la I-CSCF reenvía el mensaje de petición de Registro a la dirección de la función S-CSCF seleccionada o reenviada.

Etapa 213: Después de recibir el mensaje de petición, la S-CSCF comprueba la identidad del usuario en el mensaje y determina que el solicitador del registro es un usuario que accede a la red desde el dominio de CS e indica el sistema de autenticación soportado por el UE y el tipo de red de acceso al HSS. Por lo tanto, el HSS puede obtener los datos de autenticación correspondientes.

Etapa 214: Después de recibir la petición, el HSS determina que el usuario es un usuario de CS USIM en función de la identidad del usuario y genera un vector de autenticación quintupleto correspondiente (AV) para el usuario. Si el HSS determina que el usuario accede a la red a través de un GSM BSS en función de la red de acceso, el HSS combina la clave CK y la clave IK en una Kc, indica que el sistema de autenticación puesto en práctica por la red es el acuerdo de claves de autenticación y la conmutación de circuitos del sistema universal de telecomunicaciones móviles (AKA-UMTS-CS) y luego, reenvía el resultado a la S-CSCF.

Etapa 215: Después de recibir una respuesta de autenticación del HSS, la S-CSCF elimina el parámetro de XRES en el vector de autenticación (AV) y guarda la respuesta de autenticación. Más adelante, la S-CSCF inicia un desafío de autenticación al usuario reenviando un mensaje 401 y define el parámetro de "algoritmo" en el campo de cabecera WWW-Autenticar para "AKA-UMTS-CS" que es un sistema de autenticación de red indicado por el HSS.

Etapa 216: Después de recibir el mensaje 401 de desafío de autenticación, el RPF genera un mensaje de petición de autenticación de dominio CS correspondiente y lo envía al UE a través del BSS.

Etapa 217: En función del parámetro de autenticación recibido, el UE calcula el resultado de la autenticación y lo reenvía al RPF a través del BSS. Si la configuración de red requiere un proceso de seguridad de dominio CS, el RPF inicia un segundo registro para la red de IMS después de recibir un mensaje de "conclusión de protección de seguridad". Si el dominio de CS no requiere ningún proceso de seguridad, el RPF puede iniciar un segundo proceso de registro para la red de IMS después de recibir una respuesta de autenticación de UE desde el BSS;

Etapa 218: Después de recibir la segunda petición de Registro reenviada por la I-CSCF, la S-CSCF compara la RES (respuesta de autenticación) enviada desde el UE con la XRES (respuesta exceptuada) almacenada en la S-CSCF; si son la misma, la autenticación fue un éxito y la S-CSCF notifica al HSS del éxito del registro del usuario, descarga los datos de usuario desde el HSS y luego reenvía un mensaje 200 OK al RPF. Dependiendo de la inspección realizada con respecto a iFC, la S-CSCF puede iniciar un proceso de registro de terceros para el AS.

Etapa 219: Después de recibir el mensaje 200 OK, el RPF actualiza el estado de usuario almacenado, la información de dirección y el valor del intervalo de espera del registro y reenvía un mensaje "aceptación de actualización de posición" al UE, con la TMSI recientemente asignada transmitida en el mensaje; más adelante, el RPF envía una petición a la S-CSCF para la suscripción a la notificación del estado de registro del usuario; después de recibir la petición de suscripción, la S-CSCF responde con un mensaje NOTIFY que transmite la información de registro del usuario, incluyendo todas las IMPUs registradas que no estén prohibidas.

Etapa 2110: Después de concluir el registro de terceros en la S-CSCF, el AS recupera los datos de usuario pertinentes desde el HSS y realiza la suscripción para eventos de cambio de datos de usuario.

Forma de realización 9

En el segundo modo, el proceso de registro inicial realizado antes de que un usuario de CS móvil pueda acceder a una red de IMS se representa en la Figura 21. Es decir, el proceso para una tarjeta de USIM de un terminal 2G, para acceder a la red a través de un GSM BSS, comprende las etapas siguientes:

Etapa 221: Después de detectar la petición de actualización de posición enviada por el UE, el RPF exporta el ID requerido para el registro al dominio de IMS en función del CS del ID del usuario de CS y resuelve la dirección de la I-CSCF base, en función del nombre de dominio base exportado; más adelante, el RPF envía un mensaje de Registro de SIP a la I-CSCF para el registro en la red de IMS; el mensaje de Registro debe transmitir el parámetro extendido del campo de cabecera de Autorización, por ejemplo, "Auth-scheme", para indicar el sistema de autenticación que se soporta por el UE y obtenido por el RPF, en función de la señalización de CS recibida desde el RNC; el mensaje de Registro transmite también la información de red de acceso en el campo de cabecera de "P-acceso-red-info". En esta forma de realización, la red de acceso está en un modo de GERAN.

Etapa 222: En función de la IMPU y de la IMPI del usuario, la I-CSCF consulta al HSS para conocer el estado de registro del usuario. Si el HSS determina que el usuario es legal y no está registrado, el HSS reenvía la información de capacidad de la función S-CSCF a la I-CSCF y la I-CSCF selecciona una S-CSCF para gestionar la petición de Registro. Si el usuario es legal y está registrado, el HSS reenvía la información de dirección de S-CSCF y la I-CSCF reenvía el mensaje de petición de Registro a la dirección de la S-CSCF reenviada o seleccionada.

Etapa 223: Después de recibir el mensaje de petición de Registro desde la I-CSCF, la S-CSCF comprueba la identidad del usuario en el mensaje y determina que el solicitador de registro es un usuario que accede a la red desde un dominio de CS y envía un mensaje de petición de autenticación multimedia al HSS. El mensaje indica el sistema de autenticación soportado por el UE y el tipo de la red de acceso, de modo que el HSS pueda obtener los datos de autenticación correspondientes.

Etapa 224: Después de recibir la petición, el HSS determina que el usuario es un usuario de CS USIM en función de la identidad del usuario y genera un vector de autenticación (AV) quintupleto correspondiente para el usuario. Si el HSS determina que el usuario accede a la red a través de un GSM BSS en función de la red de acceso y el UE soporta el sistema de GSM AKA, el HSS combina las claves CK e IK en una Kc, indica que el sistema de autenticación puesto en práctica por la red es el acuerdo de claves de autenticación y conmutación de circuitos del sistema universal de telecomunicaciones móviles (AKA-GSM-CS) y a continuación, reenvía la información del usuario y el sistema de autenticación determinado a la entidad S-CSCF.

Etapa 225: Después de recibir una respuesta de autenticación desde el HSS, la S-CSCF elimina el parámetro de SRES en el vector de autenticación (AV) y guarda la respuesta de autenticación. Más adelante, la S-CSCF inicia un desafío de autenticación al usuario reenviando un mensaje 401 al RPF a través de la entidad I-CSCF y define el parámetro de "algoritmo" en el campo de cabecera WWW-Autenticar a "AKA-GSM-CS" que es un sistema de autenticación de red indicado por el HSS.

Etapa 226: Después de recibir el mensaje de desafío de autenticación 401, el RPF genera un mensaje de petición de autenticación del dominio de CS correspondiente y lo envía al UE a través del servidor BSS.

Etapa 227: En función del parámetro de autenticación recibido, el UE calcula el resultado de la autenticación y lo reenvía al RPF a través del BSS. Si la configuración de la red requiere un proceso de seguridad del dominio CS, el RPF inicia un segundo registro para la red de IMS después de recibir un mensaje de "conclusión de protección de seguridad". Si el dominio de CS no requiere ningún proceso de seguridad, el RPF puede iniciar un segundo proceso de registro para la red de IMS después de recibir una respuesta de autenticación de UE desde el BSS;

Etapa 228: Después de recibir la segunda petición de Registro reenviada por la I-CSCF, la S-CSCF compara la SRES enviada desde el UE con la SRES almacenada en la S-CSCF; si son las mismas, la autenticación ha tenido éxito y la S-CSCF notifica al HSS el éxito del registro del usuario, descarga los datos de usuario del HSS y luego, reenvía un mensaje 200 OK al RPF. Dependiendo de la inspección realizada con respecto a iFC, la S-CSCF puede iniciar un proceso de registro de terceros para el servidor AS.

Etapa 229: Después de recibir el mensaje 200 OK, el RPF actualiza el estado de usuario almacenado, la información de dirección y el valor del intervalo de espera del registro y reenvía un mensaje de "aceptación de actualización de posición" al UE, con la TMSI recientemente asignada transmitida en el mensaje; más adelante, el RPF envía una petición a la S-CSCF para la suscripción a la notificación del estado de registro del usuario; después de recibir la petición de suscripción, la S-CSCF responde con un mensaje NOTIFY que transmite la información de registro del usuario, incluyendo todas las IMPUs que no estén prohibidas.

Etapa 2210: Después de concluir el registro de terceros en la S-CSCF, el servidor AS recupera los datos de usuario pertinentes desde el HSS y realiza la suscripción para eventos de cambio de datos de usuario.

Forma de realización 10

En el segundo modo, el proceso en el que un usuario de CS móvil falla en la autenticación de la red, se representa en la Figura 22, que toma el sistema WCDMA a modo de ejemplo y simplifica el proceso de interacción con la red RAN.

Según se representa en la Figura 22, el proceso en el que una tarjeta USIM de un terminal 3G tiene fallos en la autenticación de la red, cuando se accede a la red a través de un RNS, comprende:

Etapa 231: Después de recibir una petición de autenticación, el UE realiza la autenticación de la red en función de RAND y de AUTN. Si el número de serie calculado no es aceptable para el UE, el UE calcula el denominado *token* de autenticación de fallo de sincronización (AUTS) y lo reenvía a la red, especificando la causa como fallo de sincronización.

Etapa 232: Después de recibir el AUTS desde el UE, la S-CSCF solicita los datos de autenticación del HSS de nuevo y el HSS actualiza sus propios datos en función de la gama de números de serie calculados aceptables para el UE, genera de nuevo datos de autenticación y reenvía los datos de autenticación a la S-CSCF.

Etapa 233: El UE recibe los nuevos datos de autenticación desde la S-CSCF y realiza, de nuevo, la autenticación de la red. Si la re-autenticación tiene éxito, el proceso posterior es el mismo que el proceso que sigue la autenticación inicial satisfactoria.

Forma de realización 11

En el segundo modo, el proceso de registro inicial realizado antes de que un usuario de CS móvil pueda acceder a una red de IMS se representa en la Figura 23 suponiendo que una tarjeta SIM de un terminal 2G accede a la red de IMS a través de un BSS.

Según se representa en la Figura 23, el proceso de registro inicial, puesto en práctica por una tarjeta de SIM de un terminal 2G, para acceder a la red a través de un BSS comprende las etapas siguientes:

Etapa 241: Después de detectar la petición de actualización de posición enviada por el UE, el RPF exporta el ID requerido para el registro para el dominio de IMS, en función del ID de dominio de CS del usuario de CS y resuelve la dirección de I-CSCF base en función del nombre de dominio base exportado; más adelante, el RPF envía un mensaje de Registro de SIP a la I-CSCF para el registro en la red de IMS; el mensaje de Registro debe transmitir el parámetro extendido del campo de cabecera de "Autorización" por ejemplo "auth-scheme", para indicar el sistema de autenticación que se soporta por el UE y obtenido por el RPF en función de la señalización de CS recibida desde el BSS; el mensaje de Registro transmite también la información de red de acceso en el campo de cabecera "P-acceso-red-info". En esta forma de realización, la red de acceso está en un modo 3GPP-GERAN.

Etapa 242: En función de la IMPU y de la IMPI del usuario, la I-CSCF consulta el HSS para conocer el estado de registro del usuario. Si el HSS determina que el usuario es legal y no está registrado, el HSS reenvía la información de capacidad de la función S-CSCF y la I-CSCF selecciona una S-CSCF para gestionar la petición de Registro. Si el usuario es legal y está registrado, el HSS reenvía la información de dirección de S-CSCF y la I-CSCF reenvía el mensaje de petición de Registro a la dirección de la S-CSCF reenviada o seleccionada.

Etapa 243: Después de recibir el mensaje de petición de Registro, la S-CSCF comprueba la identidad del usuario en el mensaje y determina que el solicitador de registro es un usuario que accede a la red desde un dominio de CS e indica el sistema de autenticación soportado por el UE y el tipo de la red de acceso al HSS. Por lo tanto, el HSS puede obtener los datos de autenticación correspondientes.

Etapa 244: Después de recibir la petición, el HSS determina que el usuario es un usuario de CS SIM en función de la identidad del usuario. Por lo tanto, el HSS genera un vector de autenticación (AV) tripleto correspondiente para el usuario, indica que el sistema de autenticación puesto en práctica por la red es AKA-GSM-CS y a continuación, reenvía el vector AV y el sistema de autenticación a la entidad S-CSCF.

Etapa 245: Después de recibir una respuesta de autenticación desde el HSS, la S-CSCF elimina el parámetro de XRES en el vector de autenticación (AV) y memoriza la respuesta de autenticación. Más adelante, la S-CSCF inicia un desafío de autenticación al usuario reenviando un mensaje 401 al RPF a través de la entidad I-CSCF y define el parámetro de "algoritmo" en el campo de cabecera de WWW-Autenticar en el mensaje "AKA-GSM-CS" que es un sistema de autenticación de la red indicado por el HSS.

Etapa 246: Después de recibir el mensaje de desafío de autenticación 401, el RPF genera un mensaje de petición de autenticación del dominio de CS correspondiente y lo envía al UE a través del RNC.

Etapa 247: En función del parámetro de autenticación recibido, el UE calcula el resultado de la autenticación y lo reenvía al RPF a través del servidor BSS. Si la configuración de red requiere un proceso de seguridad del dominio CS, el RPF inicia un segundo registro para la red de IMS después de recibir un mensaje de "conclusión de protección de seguridad". Si el dominio de CS no requiere ningún proceso de seguridad, el RPF puede iniciar un segundo proceso de registro para la red de IMS después de recibir una respuesta de autenticación de UE desde el BSS.

Etapa 248: Después de recibir la segunda petición de Registro reenviada por la I-CSCF, la S-CSCF compara la SRES enviada desde el UE con la RES almacenada en la S-CSCF; si son las mismas, la autenticación ha tenido éxito y la S-CSCF notifica al HSS el éxito del registro del usuario, descarga los datos de usuario desde el HSS y a continuación, reenvía un mensaje 200 OK al RPF. Dependiendo de la inspección realizada con respecto a iFC, la S-CSCF puede iniciar un proceso de registro de terceros para el servidor AS.

Etapa 249: Después de recibir el mensaje 200 OK, el RPF actualiza el estado de usuario almacenado, la información de dirección y el valor del intervalo de espera del registro y reenvía un mensaje de "aceptación de actualización de posición" al UE, con la TMSI recientemente asignada transmitida en el mensaje; más adelante, el RPF envía una petición a la S-CSCF para la suscripción de la notificación del estado de registro del usuario; después de recibir la petición de suscripción, la S-CSCF responde con un mensaje NOTIFY que transmite la información de registro del usuario, incluyendo todas las IMPUs registradas que no estén prohibidas.

Etapa 2410: Después de concluir el registro de terceros en la S-CSCF, el servidor AS recupera los datos de usuario pertinentes desde el HSS y realiza la suscripción al evento de cambio de datos de usuario.

Forma de realización 12

En el segundo modo, el proceso de registro inicial realizado antes de que un usuario de CS móvil pueda acceder a una red de IMS, se representa en la Figura 24. Suponiendo que el proceso se aplica a un sistema de CDMA, el proceso de registro inicial realizado por una tarjeta R-UIM de un terminal CDMA 2G para acceder a la red a través de un BSS comprende las etapas siguientes:

Etapa 251: Después de detectar la petición de actualización de posición enviada por el UE, el RPF exporta el ID requerido para el registro para el dominio de IMS en función del identificador ID del dominio de CS del usuario de CS y resuelve la dirección de la I-CSCF base en función del nombre de dominio base exportado; más adelante, el RPF envía un mensaje de Registro de SIP a la I-CSCF para el registro en la red de IMS; el mensaje de Registro debe transmitir el parámetro extendido del campo de cabecera de Autorización, por ejemplo "auth-scheme", para indicar el sistema de autenticación que se soporta por el UE y obtenido por el RPF en función de la señalización de CS recibida desde el BSS; el mensaje de Registro transmite también la información de red de acceso en el campo de cabecera "P-acceso-red-info". En esta forma de realización, la red de acceso está en un modo 3GPP-CDMA2000.

Etapa 252: En función de la IMPU y de la IMPI del usuario, la I-CSCF consulta el HSS para conocer el estado de registro del usuario después de recibir el mensaje de Registro. Si el HSS determina que el usuario es legal y no está registrado, el HSS reenvía la información de capacidad de S-CSCF a la I-CSCF y la I-CSCF selecciona una S-CSCF para gestionar la petición de Registro en función de la información de capacidad de la S-CSCF. Si el usuario es legal y está registrado, el HSS reenvía la información de dirección de S-CSCF y la I-CSCF reenvía el mensaje de petición de Registro a la dirección de S-CSCF reenviada o seleccionada.

Etapa 253: Después de recibir el mensaje de petición de Registro, la S-CSCF comprueba la identidad del usuario en el mensaje y determina que el solicitador de registro es un usuario que accede a la red desde un dominio de CS e indica el

sistema de autenticación soportado por el UE y el tipo de la red de acceso al HSS. Por lo tanto, el HSS puede obtener los datos de autenticación correspondientes.

Etapa 254: Después de recibir la petición, el HSS determina que el usuario es un usuario de CS R-UIM en función de la identidad del usuario. Por lo tanto, el HSS genera un vector de autenticación (AV) dupleto correspondiente para el usuario, indica que el sistema de autenticación puesto en práctica por la red es AKA-CDMA-CS y a continuación, reenvía el vector AV y el sistema de autenticación a la S-CSCF.

Etapa 255: Después de recibir una respuesta de autenticación desde el HSS, la S-CSCF elimina el parámetro Auth-U en el vector de autenticación (AV) y memoriza la respuesta de autenticación. Más adelante, la S-CSCF inicia un desafío de autenticación al usuario reenviando un mensaje 401 al RPF a través de la entidad I-CSCF y define el parámetro de "algoritmo" en el campo de cabecera de WWW-Autenticar en el mensaje a "AKA-CDMA-CS" que es un sistema de autenticación de la red indicado por el HSS.

Etapa 256: Después de recibir el mensaje de desafío de autenticación 401, el RPF genera un mensaje de petición de autenticación del dominio de CS correspondiente y lo envía al UE a través del RNC.

Etapa 257: En función del parámetro de autenticación recibido, el UE calcula el resultado de la autenticación y lo reenvía al RPF a través del servidor BSS. Si la configuración de la red requiere un proceso de seguridad del dominio de CS, el RPF inicia un segundo registro para la red de IMS después de recibir un mensaje de "conclusión de protección de seguridad". Si el dominio de CS no requiere ningún proceso de seguridad, el RPF puede iniciar un segundo proceso de registro para la red de IMS después de recibir una respuesta de autenticación de UE desde el BSS.

Etapa 258: Después de recibir la segunda petición de Registro reenviada por la I-CSCF, la S-CSCF compara el parámetro Auth-U enviado desde el UE con el Auth-U almacenado en la S-CSCF; si son los mismos, la autenticación se realizó con éxito y la S-CSCF notifica al HSS el éxito del registro del usuario, descarga los datos de usuario desde el HSS y a continuación, reenvía un mensaje 200 OK al RPF. Dependiendo de la inspección realizada con respecto a iFC, la S-CSCF puede iniciar un proceso de registro de terceros para el servidor AS.

Etapa 259: Después de recibir el mensaje 200 OK, el RPF actualiza el estado de usuario almacenado, la información de dirección y el valor del intervalo de espera del registro y reenvía un mensaje de "aceptación de actualización de posición" al UE; más adelante, el RPF envía una petición a la S-CSCF para la suscripción de la notificación del estado de registro del usuario; después de recibir la petición de suscripción, la S-CSCF responde con un mensaje NOTIFY que transmite la información de registro del usuario, incluyendo todas las IMPUs registradas que no estén prohibidas.

Etapa 2510: Después de concluir el registro de terceros en la S-CSCF, el servidor AS recupera los datos de usuario pertinentes desde el HSS y realiza la suscripción para evento de cambio de datos de usuario.

Forma de realización 13

En el segundo modo, el proceso de de-registro iniciado por el usuario cuando un usuario de CS móvil accede a una red de IMS, según se representa en la Figura 25, suponiendo que el RPF está combinado con la P-CSCF.

Según se representa en la Figura 25, el proceso de registro inicial iniciado por una tarjeta USIM de un terminal 3G para acceder a la red a través de un BSS comprende las etapas siguientes:

Etapa 261: Cuando se detecta un evento de desconexión de un usuario de CS, el RPF puede iniciar un de-registro para la red de IMS en nombre del usuario. Los parámetros son los mismos que los existentes en el registro inicial, con la excepción de que el campo "expira" después del campo "Contacto" se pone a 0, lo que significa que el usuario necesita un de-registro. En función del nombre de dominio base del usuario, el RPF resuelve la dirección de la I-CSCF base. Más adelante, el RPF envía un mensaje de Registro de SIP.

Etapa 262: En función de la IMPU y la IMPI del usuario, la I-CSCF consulta al HSS para conocer el estado de registro del usuario. Si el usuario es legal y está registrado, el HSS reenvía la información de la dirección de S-CSCF; la I-CSCF reenvía el mensaje de petición de Registro a la S-CSCF reenviada o seleccionada.

Etapa 263: Puesto que el valor del campo "expira" de la petición es 0, la S-CSCF conoce que el usuario necesita un de-registro. Por lo tanto, la S-CSCF notifica al HSS la actualización del estado de registro del usuario, es decir, modifica el estado de registro del usuario al estado de-registrado y reenvía un mensaje 200 OK al RPF.

Etapa 264: Después de recibir el mensaje 200 OK, el RPF borra la información relacionada con el usuario, memorizada en el RPF, con lo que se concluye el proceso de de-registro del usuario.

En conclusión, la solución técnica dada a conocer por la presente invención permite a un usuario de CS móvil registrarse en una red de IMS, de modo que el usuario de CS pueda disfrutar de servicios de IMS ricos en contenido. Las formas de

realización de la presente invención hacen viable para un operador unificar y simplificar la red de núcleo y reducir efectivamente los gastos de explotación.

Aunque la presente invención ha sido descrita a través de formas de realización a modo de ejemplo, la invención no está limitada a dichas formas de realización. Es evidente para los expertos en esta materia la facilidad para realizar varias modificaciones y variaciones en la invención sin desviarse, por ello, del alcance de protección de la invención. La invención está prevista para cubrir las modificaciones y variaciones a condición de que caigan dentro del alcance de protección definido por las reivindicaciones adjuntas o sus equivalentes.

REIVINDICACIONES

1. Un sistema para un usuario de Circuitos Conmutados (CS) móviles para acceder a una red de subsistema multimedia IP (IMS), que comprende la red de IMS para proporcionar servicios de IMS y una red de acceso de CS, caracterizado por comprender, además:

una entidad de Función de Proxy de Registro (RPF) que comprende, además, una primera interfaz para la comunicación con la red de IMS y una segunda interfaz para la comunicación con la red de acceso de CS y adaptada para establecer una correspondencia, o mapeado, de un evento de registro de CS, que tiene su origen en el usuario de CS móvil, a través de la segunda interfaz, con un evento de registro de IMS e iniciar el registro para la red de IMS a través de la primera interfaz en nombre del usuario de CS móvil;

en donde la iniciación del registro para la red de IMS a través de la primera interfaz, en nombre del usuario de CS móvil, comprende:

la entidad de RPF, adaptada para enviar el evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de realizar el registro de IMS para el usuario de CS móvil directamente sin necesidad de la autenticación del usuario de CS móvil y la conclusión del proceso de registro, si la entidad de red de IMS determina que el registro se inicie por el usuario de CS móvil (131, 132, 141, 142) y el usuario de CS móvil está autenticado en un HLR de forma satisfactoria o

la entidad de RPF, adaptada para enviar el evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de la autenticación del usuario de CS móvil y de realizar el registro de IMS para el usuario de CS móvil en función de la información transmitida en el evento de registro de IMS mapeado y concluir el proceso de registro, si la entidad de red de IMS determina que el registro se inicie por el usuario de CS móvil (201, 211, 221, 241, 251).

2. El sistema según la reivindicación 1, en donde la entidad de RPF comprende:

una unidad de detección de eventos de registro, adaptada para detectar el evento de registro de CS iniciado por el usuario de CS móvil a través de la segunda interfaz;

una unidad de mapeado, adaptada para poner en correspondencia el evento de registro detectado por la unidad de detección de eventos de registro con el evento de registro de IMS y

una unidad de registro de IMS, adaptada para el registro para la red de IMS en nombre del usuario de CS móvil, a través de la primera interfaz, en función del resultado de mapeado de la unidad de mapeado.

3. El sistema según la reivindicación 2, en donde la unidad de mapeado comprende, además, una unidad de mapeado de identidades, adaptada para poner en correspondencia el ID de un dominio de CS del usuario de CS móvil con un ID de dominio de IMS, en función de un modo de mapeado predeterminado.

4. El sistema según la reivindicación 2, en donde la entidad de RPF comprende al menos una de entre:

una unidad de autenticación de IMS, adaptada para iniciar la autenticación para un dominio de IMS en nombre del usuario de CS móvil;

una unidad de suscripción de eventos de registro de usuario, adaptada para la suscripción a los eventos de registro de usuarios en nombre del usuario de CS móvil;

una unidad de iniciación de re-registro, adaptada para re-registrar a la red de IMS en nombre del usuario de CS móvil o gestionar el re-registro iniciado por la red de IMS para el usuario de CS móvil;

una unidad de de-registro de usuario, adaptada para de-registrar desde la red de IMS en nombre del usuario de CS móvil o gestionar el proceso de de-registro iniciado por la red de IMS para el usuario de CS móvil y

una unidad de suscripción de eventos de transferencia de usuarios, adaptada para realizar la suscripción a, y la notificación de, eventos de transferencia de usuarios del usuario de CS móvil iniciados por la entidad de red de IMS.

5. El sistema según la reivindicación 1, 2, 3 o 4, en donde la entidad de RPF comprende una tercera interfaz para comunicarse con una base de datos de suscripción de CS del usuario de CS móvil y mediante la tercera interfaz, la entidad de RPF realiza el registro y la autenticación en el dominio de CS, en nombre del usuario de CS móvil.

6. Un método de registro para habilitar a un usuario de Circuitos Conmutados (CS) móvil para acceder a una red de subsistema multimedia de IP (IMS), caracterizado porque comprende:

el mapeado, por una entidad de Función de Proxy de Registro (RPF), de un evento de registro de CS, con un evento de registro de IMS después de detectar el evento de registro de CS iniciado por el usuario de CS móvil y

la iniciación, por la entidad de RPF, de un proceso de registro para la red de IMS mediante el evento de registro de IMS;

en donde la iniciación del proceso de registro para la red de IMS, a través del evento de registro de IMS, comprende:

el envío, por la entidad de RPF, del evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS está realizando el registro de IMS para el usuario de CS móvil directamente sin necesidad de la autenticación del usuario de CS móvil y la conclusión del proceso de registro, si la entidad de red de IMS determina que el registro se inicie por el usuario de CS móvil (131, 132, 141, 142) y el usuario de CS móvil es autenticado en un HLR de forma satisfactoria,

o

el envío, por la entidad de RPF, del evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS está realizando la autenticación del usuario de CS móvil y la realización del registro de IMS para el usuario de CS móvil en función de la información transmitida en el evento de registro de IMS mapeado y la conclusión del proceso registro, si la entidad de red de IMS determina que el registro se inicie por el usuario de CS móvil (201, 211, 221, 241, 251).

7. El método según la reivindicación 6, en donde la etapa de mapeado del evento de registro de CS con el evento de registro de IMS comprende:

el mapeado, por la entidad de RPF, de un evento de activación para un evento de registro inicial de IMS después de detectar el evento de activación del usuario de CS móvil o

el mapeado, por la entidad de RPF, de un evento de actualización de posición inicial con un evento de registro inicial de IMS, después de detectar el evento de actualización de posición inicial cuando el usuario de CS móvil realiza una itinerancia a una nueva zona de posición o

el mapeado, por la entidad de RPF, de un evento de actualización de posición periódica para un evento de re-registro de IMS, después de detectar el evento de actualización de posición periódica del usuario de CS móvil o

el mapeado por la entidad de RPF, de un evento de desconexión de usuario con un evento de de-registro de red de IMS después de detectar el evento de desconexión del usuario de CS móvil.

8. El método según la reivindicación 6, en donde la etapa de mapeado del evento de registro de CS con el evento de registro de IMS comprende, además: convertir un ID de dominio de CS del usuario de CS móvil en un ID de dominio de IMS y/o el mapeado de los parámetros de dominio de CS con los parámetros de dominio de IMS.

9. El método según la reivindicación 8, en donde el proceso de convertir el ID de dominio de CS del usuario de CS móvil en el ID de dominio de IMS, comprende:

la generación de un nombre de dominio base de dominio de IMS correspondiente en función de un código de red móvil y un código del país del móvil en la Identidad Internacional de Abonado a un Móvil (IMSI) del usuario de CS móvil y/o

la generación de una Identidad Pública Multimedia IP (IMPU) temporal en función de la IMSI del usuario de CS móvil y/o

la obtención de una IMPU por defecto reenviada como la IMPU por defecto del usuario de CS móvil en la red de IMS después de registrar el usuario de CS móvil para la red de IMS.

10. El método, según la reivindicación 6, que comprende, además:

la iniciación, por la entidad de RPF, de un proceso de registro de CS para el usuario de CS móvil para el Registro de Posición Base (HLR) a través de una interfaz con el HLR y el mapeado del evento de registro de CS con el evento de registro de IMS después de que se concluya el proceso de registro de CS.

11. El método según la reivindicación 6, en donde el proceso de la entidad de red de IMS determina que el registro se inicie por el usuario de CS móvil en la etapa de iniciación del proceso de registro para la red de IMS a través del evento de registro de IMS, comprende:

la identificación, por la entidad de red de IMS, de que un solicitador de registro es el usuario de CS móvil en función de una identidad de usuario en una petición de Registro o la identificación, por la entidad de red de IMS, de que un solicitador de registro es el usuario de CS móvil en función de los valores de parámetros específicos o una combinación de diferentes valores de parámetros en una petición de Registro.

12. El método según la reivindicación 6, en donde la etapa de autenticación del usuario de CS móvil y la realización del registro de IMS para el usuario de CS móvil por la entidad de red de IMS en función de la información transmitida en el evento de registro de IMS mapeado, comprende:

mediante una Función de Control de Sesión de Llamadas–Servidor (S-CSCF) en la red de IMS, el envío de un mensaje de petición a un Servidor de Abonados Base (HSS) para obtener información de autenticación del usuario de CS móvil, por el HSS, la generación de un vector de autenticación (AV) para el usuario de CS móvil, en función del mensaje de petición recibido, la determinación de un sistema de autenticación soportado por la red y el reenvío del sistema de autenticación a la S-CSCF y

mediante la S-CSCF, la interacción con el usuario de CS móvil para realizar la autenticación del usuario de CS móvil en función del vector AV reenviado por el HSS y el sistema de autenticación soportado por la red, que permite al usuario de CS móvil registrarse para la red de IMS después del éxito de la autenticación y prosiguiendo con el registro para el usuario de CS móvil.

13. El método según la reivindicación 12, en donde la etapa de mapeado del evento de registro de CS con el evento de registro de IMS comprende:

mediante la entidad de RPF, el mapeado de capacidades de autenticación detectadas, soportadas por el usuario de CS móvil, con parámetros en un mensaje de Registro del Protocolo de Iniciación de Sesión (SIP) y la iniciación del registro para la red de IMS.

14. El método según la reivindicación 6, en donde la etapa de iniciar el proceso de registro para la red de IMS a través del evento de registro de IMS comprende, además:

mediante las entidades de red de IMS, la actualización de información de estado de registro del usuario de CS móvil y el marcado del usuario de CS móvil como registrado después de concluir el proceso de registro de IMS para el usuario de CS móvil.

15. El método según cualquiera de las reivindicaciones 6 a 10, en donde el método comprende al menos una de entre las operaciones siguientes después de que el usuario de CS móvil se registre con éxito en la red de IMS:

mediante la entidad de RPF, la suscripción a los eventos de registro de usuario en nombre del usuario de CS móvil;

mediante la entidad de RPF, el re-registro para la red de IMS en nombre del usuario de CS móvil;

mediante la entidad de RPF, la operación de de-registro desde la red de IMS en nombre del usuario de CS móvil;

mediante la entidad de RPF, la gestión de de-registro para el usuario de CS móvil iniciado por la red de IMS;

mediante la entidad de RPF; la gestión de re-registro para el usuario de CS móvil iniciado por la red de IMS y

mediante la entidad de RPF, la realización de la suscripción a, y la notificación de, los eventos de transferencia de usuarios del usuario de CS móvil iniciado mediante la entidad de red de IMS.

16. Una entidad de Función de Proxy de Registro (RPF), caracterizada por comprender una primera interfaz para comunicación con una red de subsistema multimedia IP (IMS) y una segunda interfaz para la comunicación con una red de acceso de circuitos conmutados (CS) y que comprende, concretamente:

una unidad de detección de eventos de registro, adaptada para detectar un evento de registro de CS iniciado por un usuario de CS móvil a través de la segunda interfaz;

una unidad de mapeado, adaptada para efectuar la puesta en correspondencia del evento de registro de CS detectado por la unidad de detección de eventos de registro con un evento de registro de IMS y

una unidad de registro de IMS, adaptada para efectuar el registro a la red de IMS, en nombre del usuario de CS móvil, a través de la primera interfaz, en función del resultado del mapeado de la unidad de mapeado;

en donde el registro para la red de IMS, en nombre del usuario de CS móvil, a través de la primera interfaz, comprende:

la entidad de RPF, adaptada para enviar el evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de realizar el registro de IMS para el usuario de CS móvil directamente sin necesidad de la autenticación del usuario de CS móvil y la conclusión del proceso de registro, si la entidad de red de IMS determina que el registro se inicie por el usuario de CS móvil (131, 132, 141, 142) y el usuario de CS móvil es objeto de autenticación en un HLR de forma satisfactoria

o

la entidad de RPF, adaptada para enviar el evento de registro de IMS mapeado a una entidad de red de IMS, en donde la entidad de red de IMS es capaz de la autenticación del usuario de CS móvil y la realización del registro de IMS para el usuario de CS móvil, en función de la información transmitida en el evento de registro de IMS mapeado y la conclusión del proceso de registro, si la entidad de red de IMS determina que el registro se inicie por el usuario de CS móvil (201, 211, 221, 241, 251).

17. El aparato según la reivindicación 16, en donde la unidad de mapeado comprende, además, una unidad de mapeado de identidades, adaptada para poner en correspondencia un ID de dominio de CS del usuario de CS móvil con un ID de dominio de IMS, en función de un modo de mapeado predeterminado.

18. El aparato según la reivindicación 16, que comprende al menos una de entre:

una unidad de autenticación de IMS, adaptada para iniciar la autenticación para un dominio de IMS en nombre del usuario de CS móvil;

una unidad de suscripción de evento de registro de usuario, adaptada para la suscripción a eventos de registro de usuarios en nombre del usuario de CS móvil;

una unidad de iniciación de re-registro, adaptada para el re-registro para la red de IMS en nombre del usuario de CS móvil o gestionar el re-registro iniciado por la red de IMS para el usuario de CS móvil;

una unidad de de-registro de usuarios, adaptada para el de-registro desde la red de IMS en nombre del usuario de CS móvil o gestionar el de-registro iniciado por la red de IMS para el usuario de CS móvil y

una unidad de suscripción de eventos de transferencia de usuarios, adaptada para realizar la suscripción a, y la notificación de, los eventos de transferencia de usuarios del usuario de CS móvil iniciado mediante la entidad de red de IMS.

19. El aparato según la reivindicación 16, 17 o 18, que comprende una tercera interfaz para la comunicación con una base de datos de suscripción de CS del usuario de CS móvil, en donde la entidad de RPF realiza el registro y la autenticación para el dominio de CS en nombre del usuario de CS móvil a través de la tercera interfaz.

20. El aparato según la reivindicación 16, 17 o 18, en donde la entidad de RPF se establece en la entidad de MSC/VLR que está localizada en el dominio de CS.

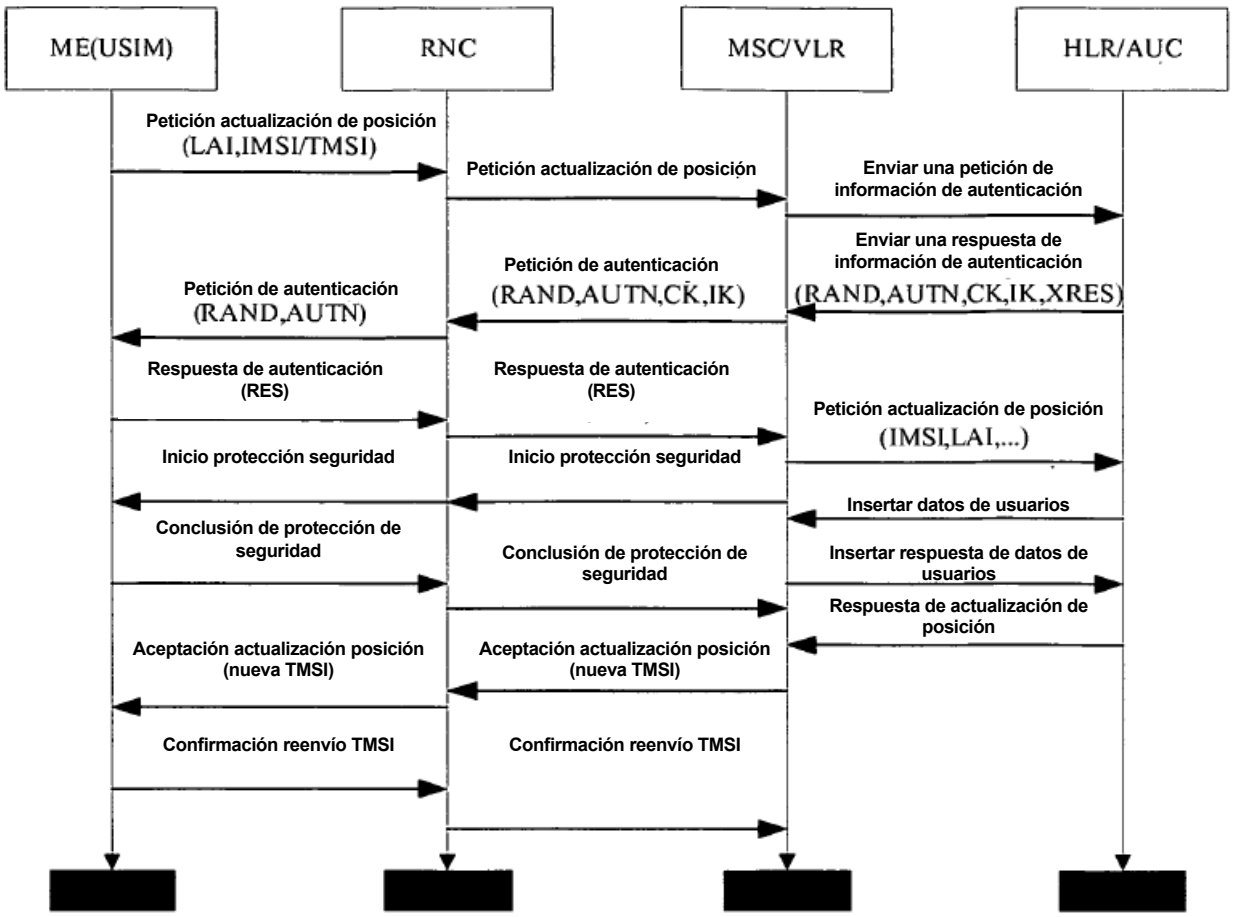


Figura 1

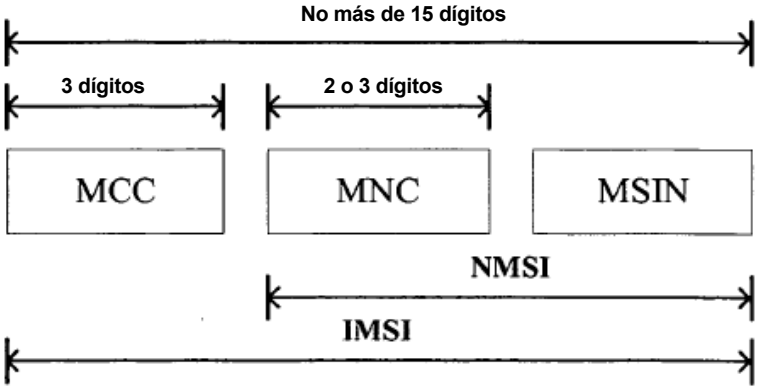


Figura 2

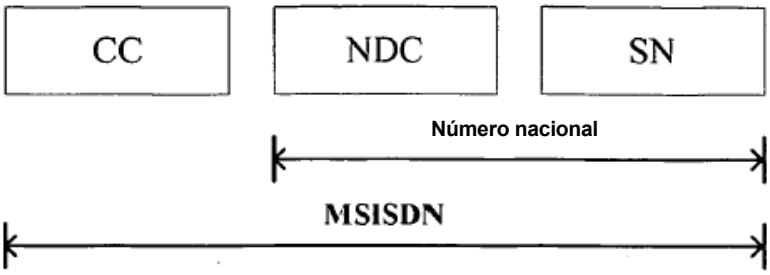


Figura 3

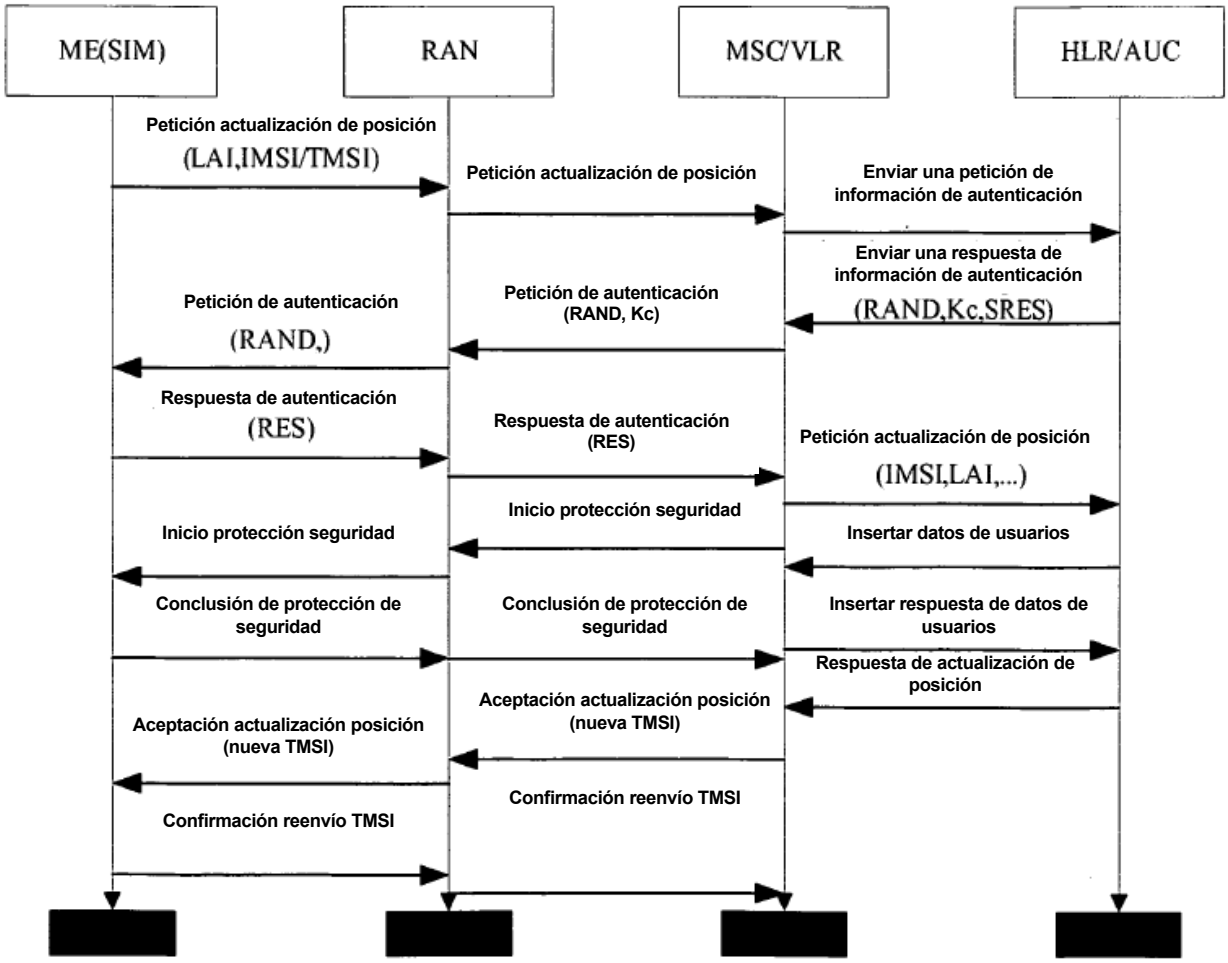


Figura 4

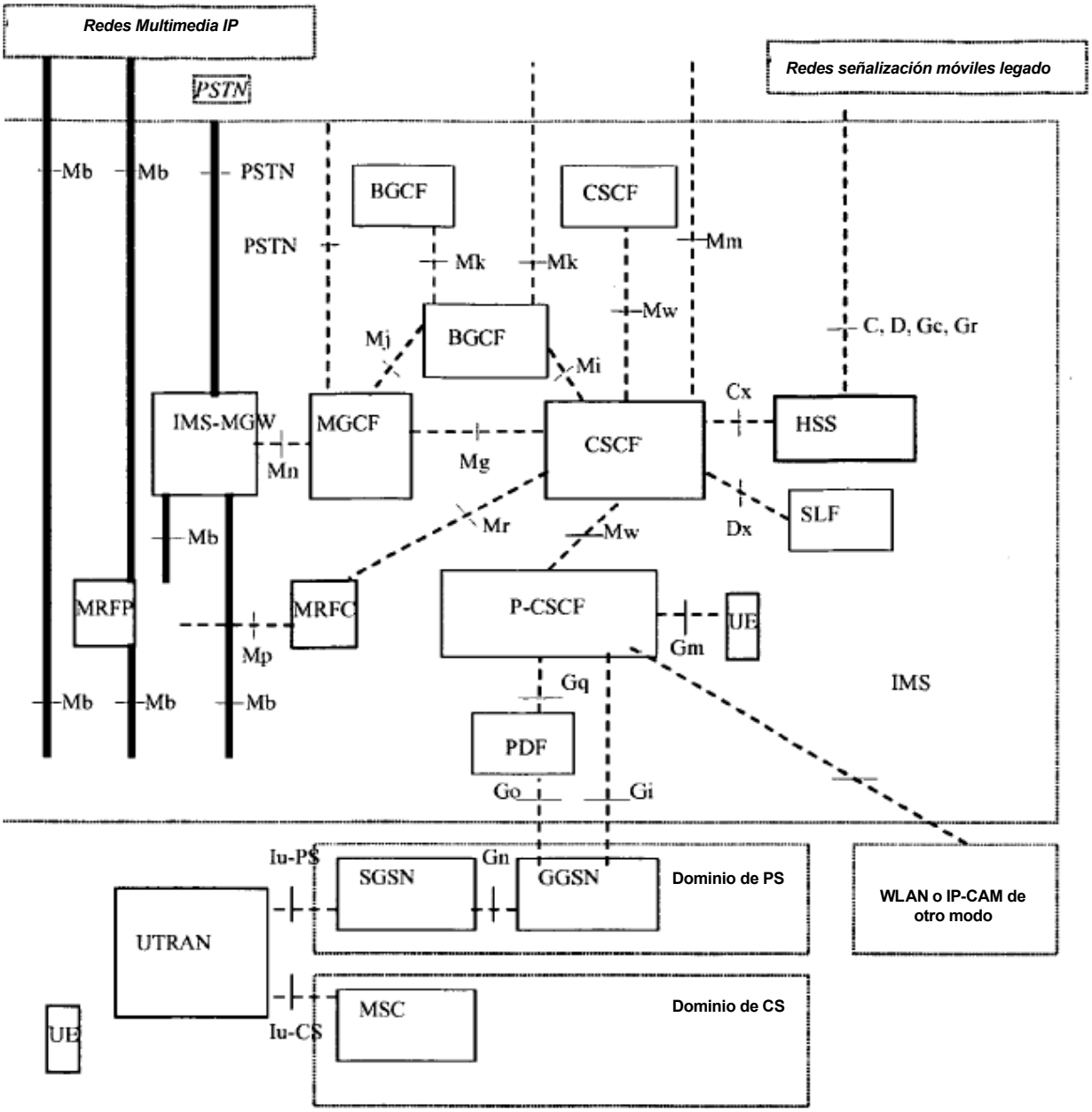


Figura 5

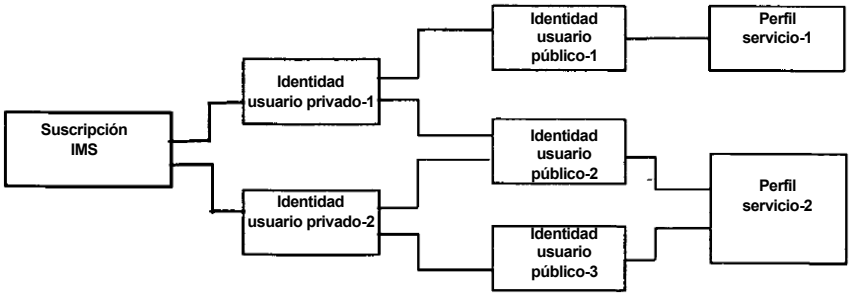


Figura 6

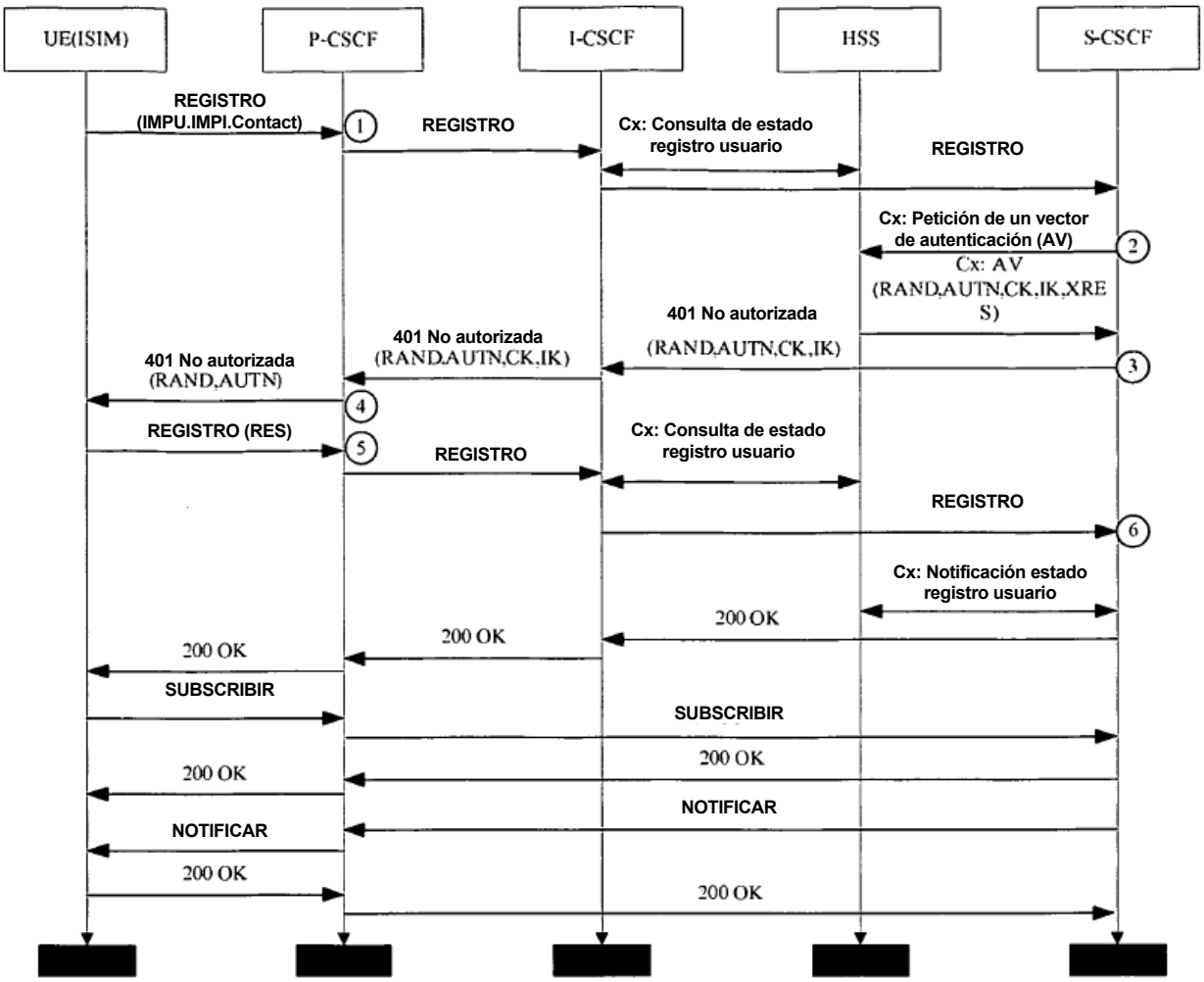


Figura 7

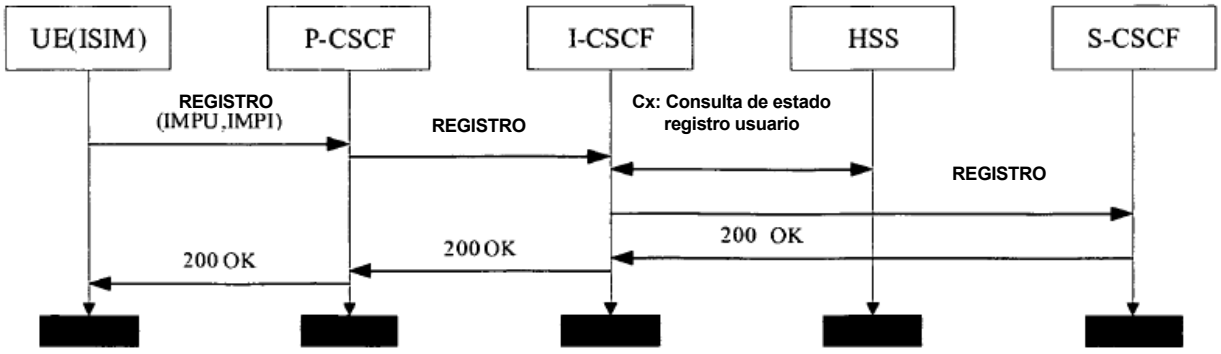


Figura 8

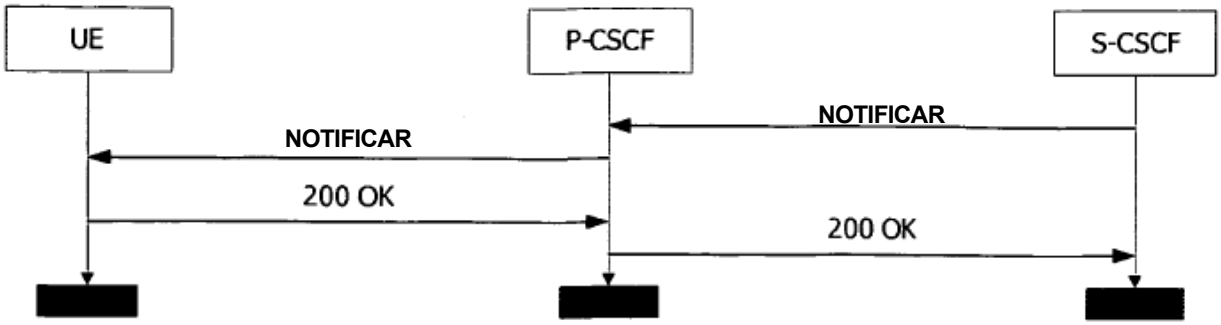


Figura 9

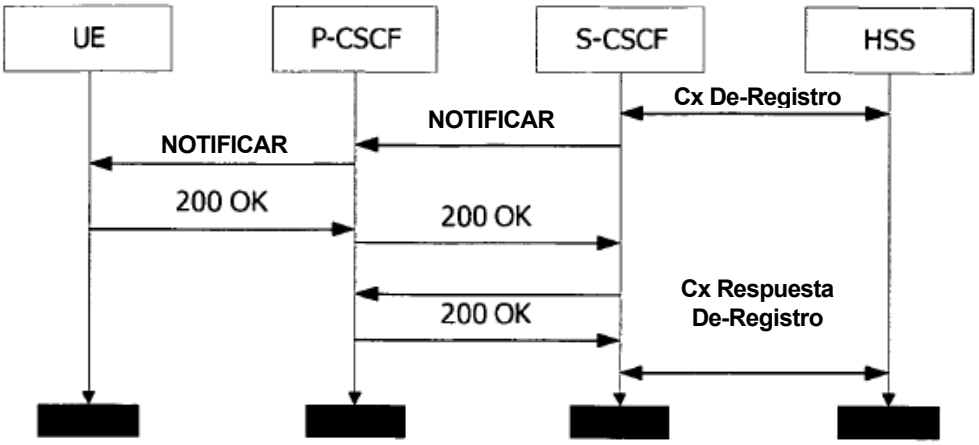


Figura 10

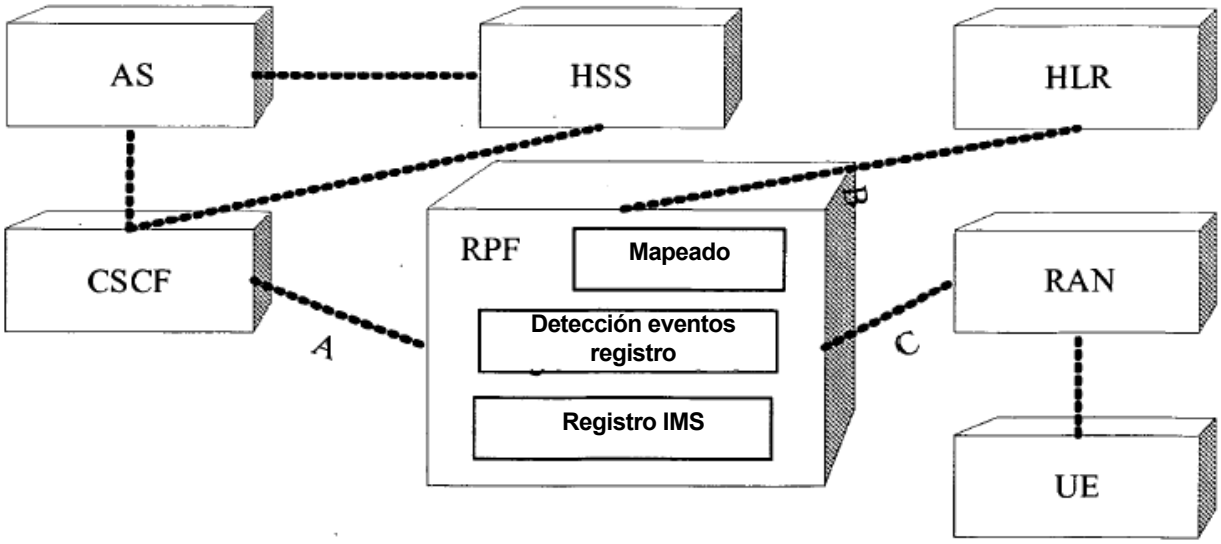


Figura 11

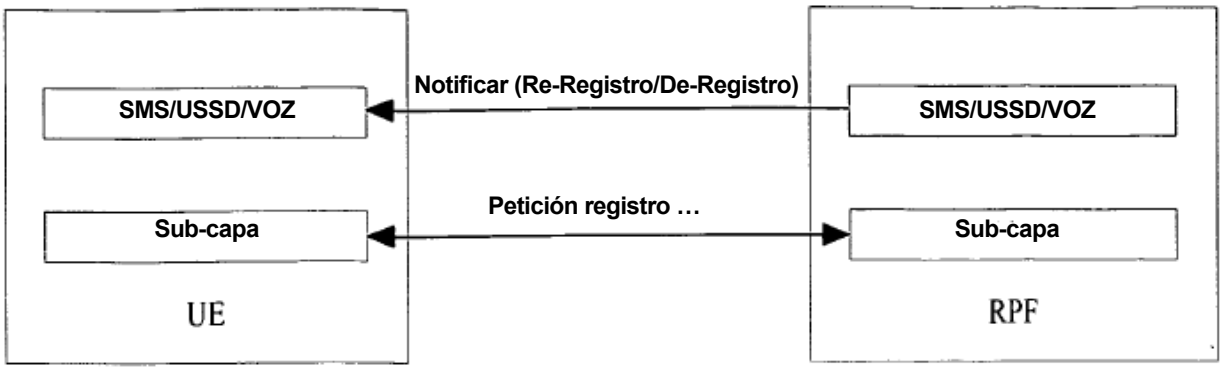


Figura 12

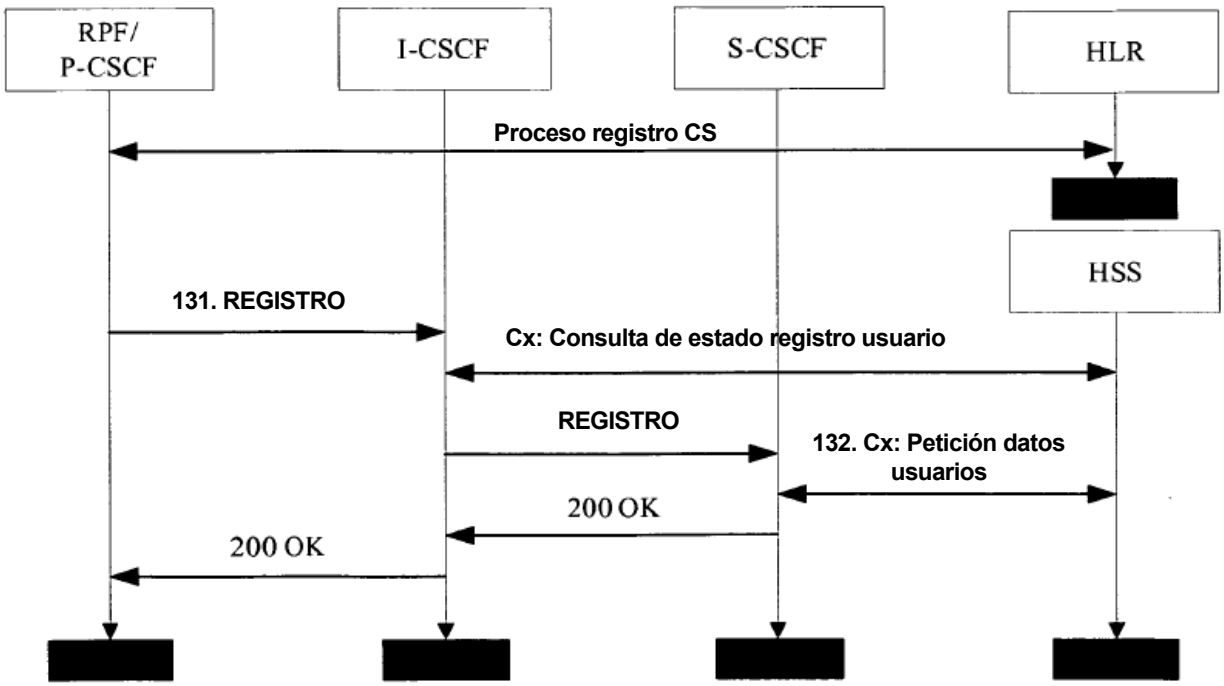


Figura 13

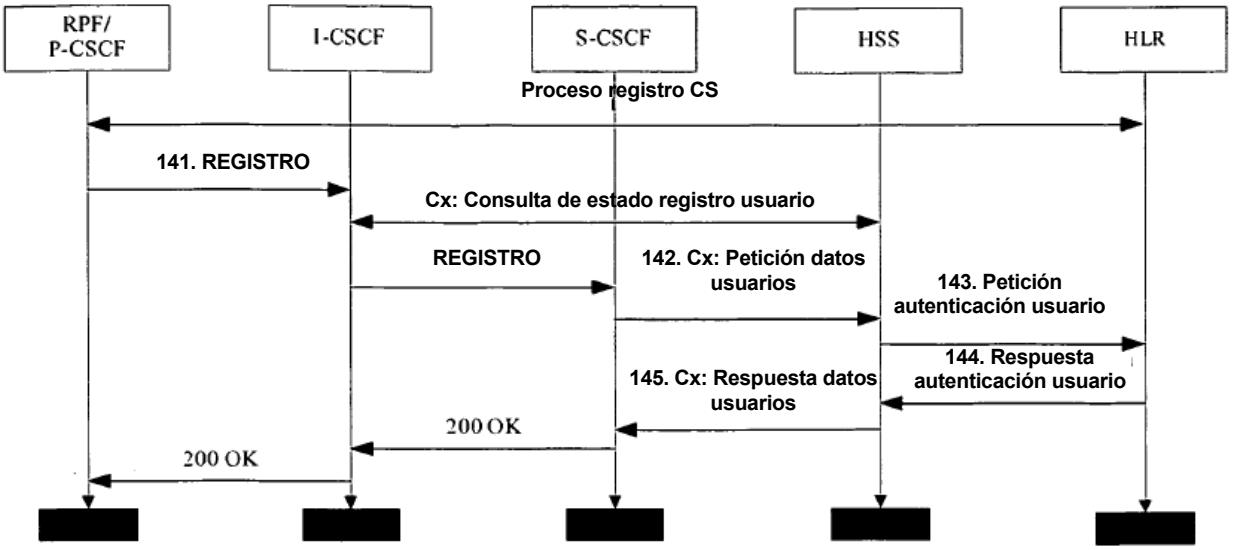


Figura 14

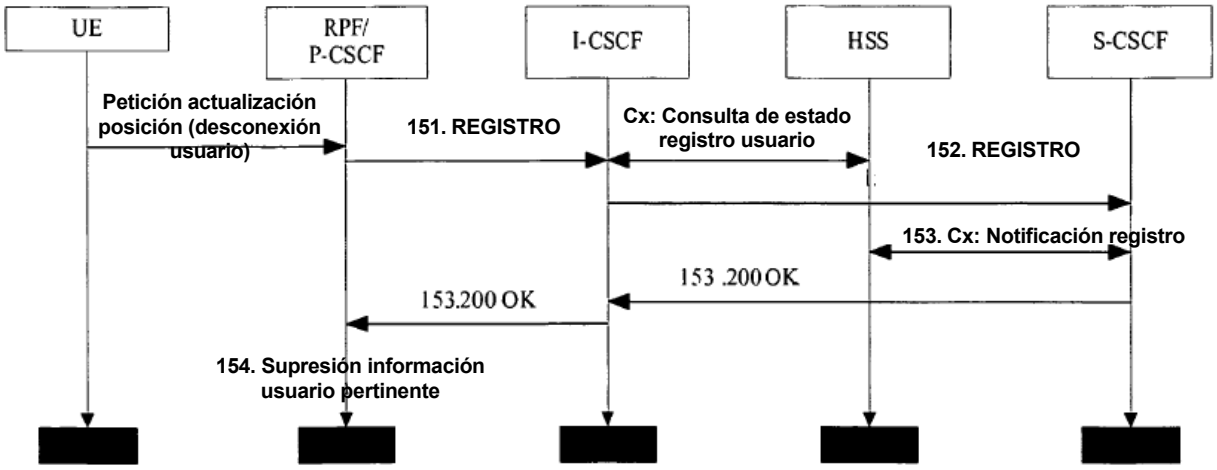


Figura 15

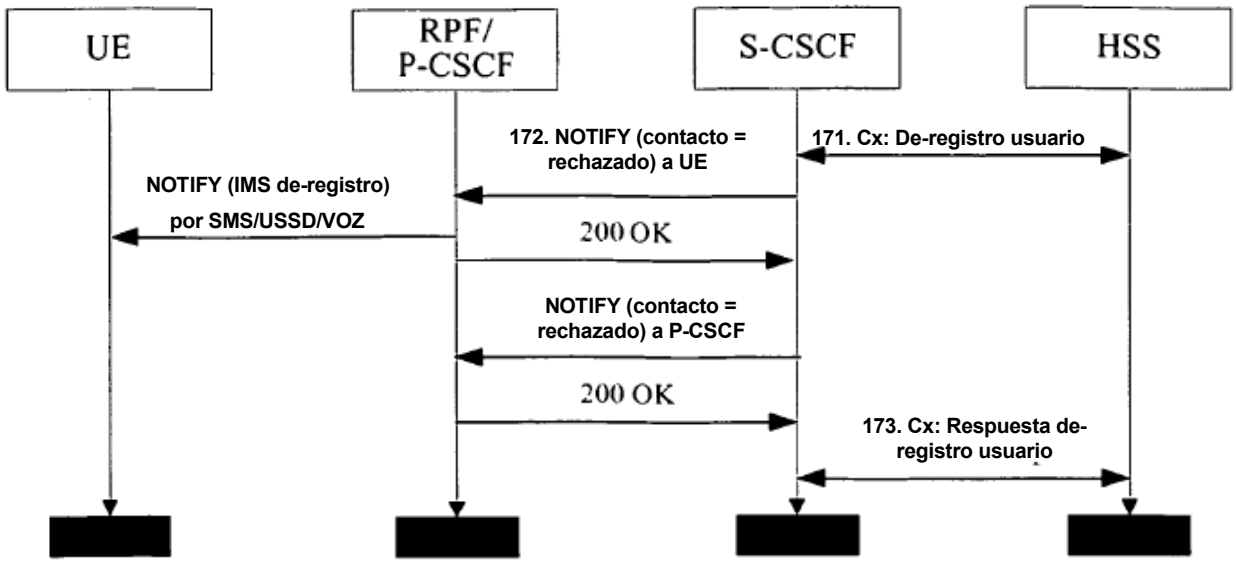


Figura 16

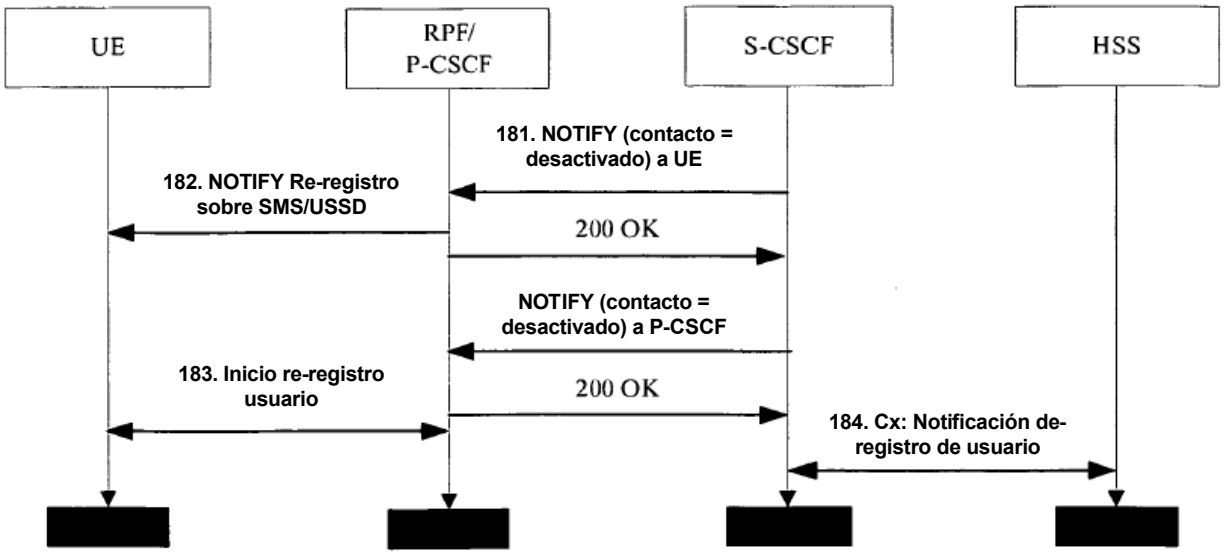


Figura 17

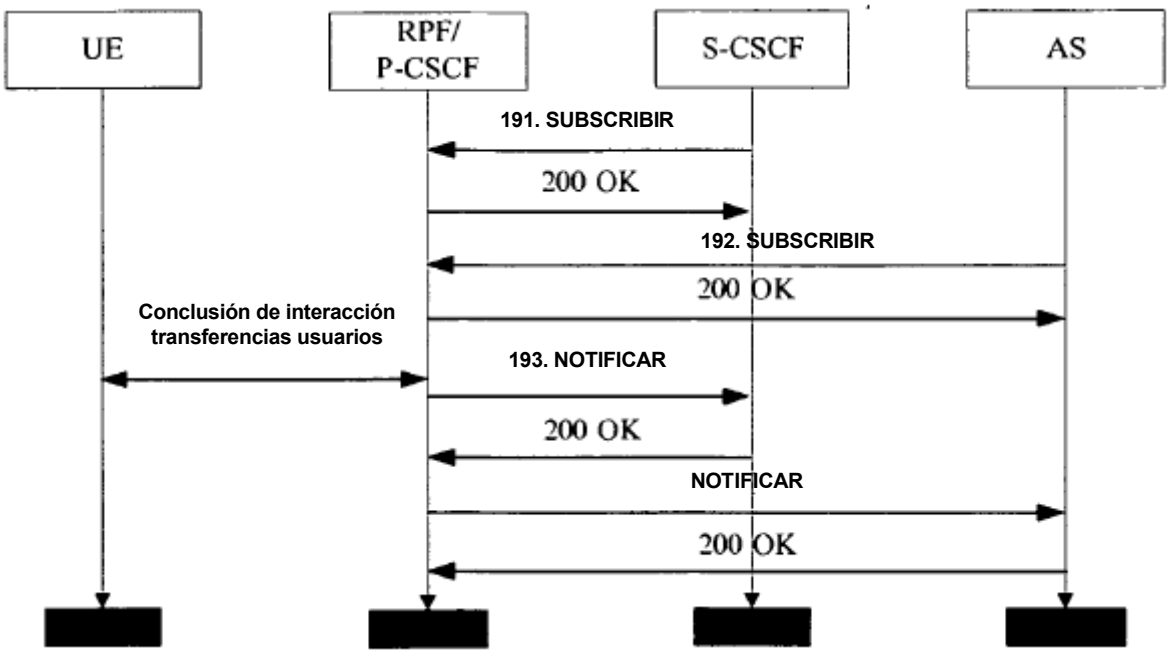

UE
RPF/
P-CSCF
S-CSCF
AS
191. SUBSCRIBIR
200 OK
192. SUBSCRIBIR
200 OK
Conclusión de interacción
transferencias usuarios
193. NOTIFICAR
200 OK
NOTIFICAR
200 OK

Figura 18

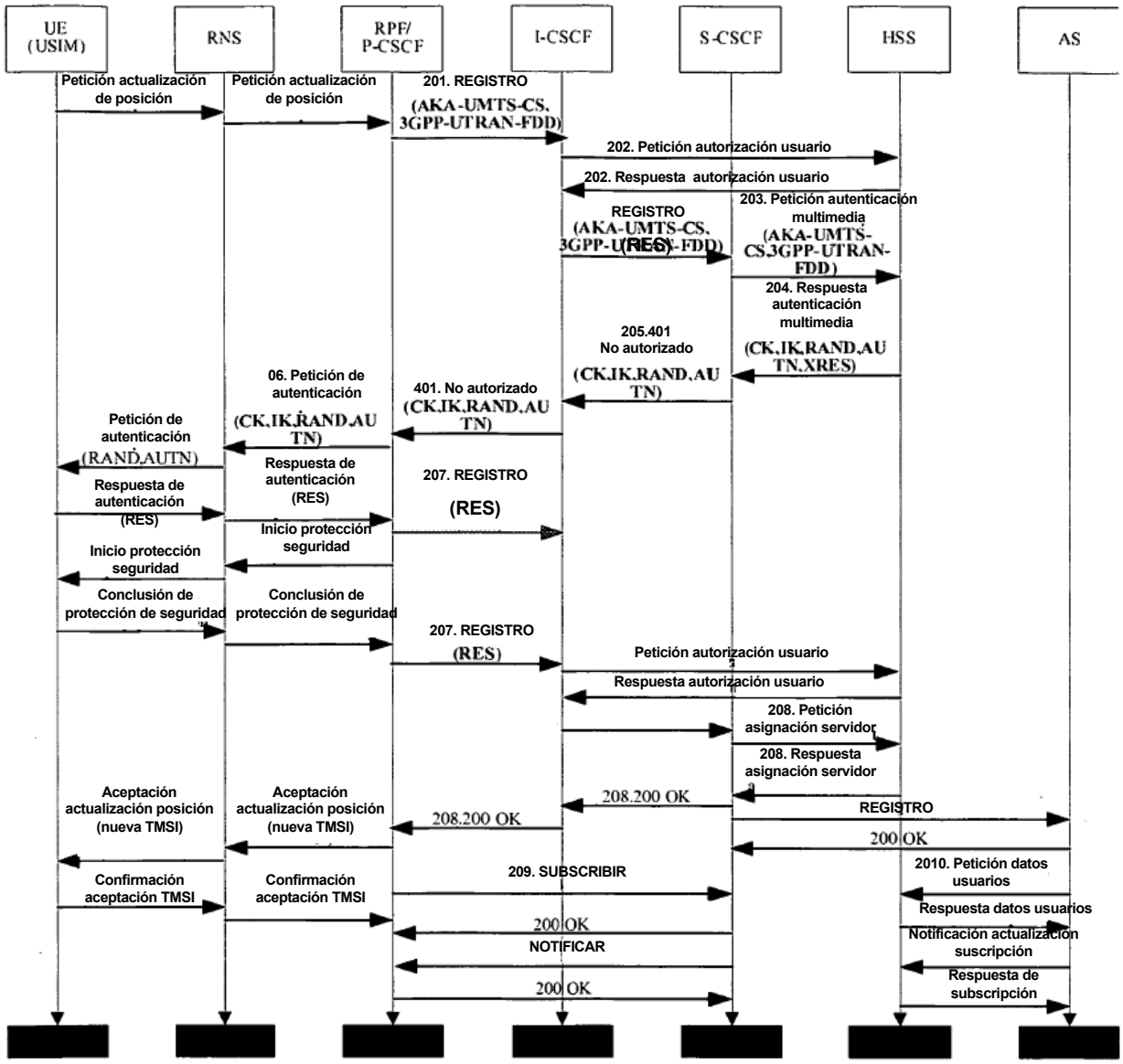
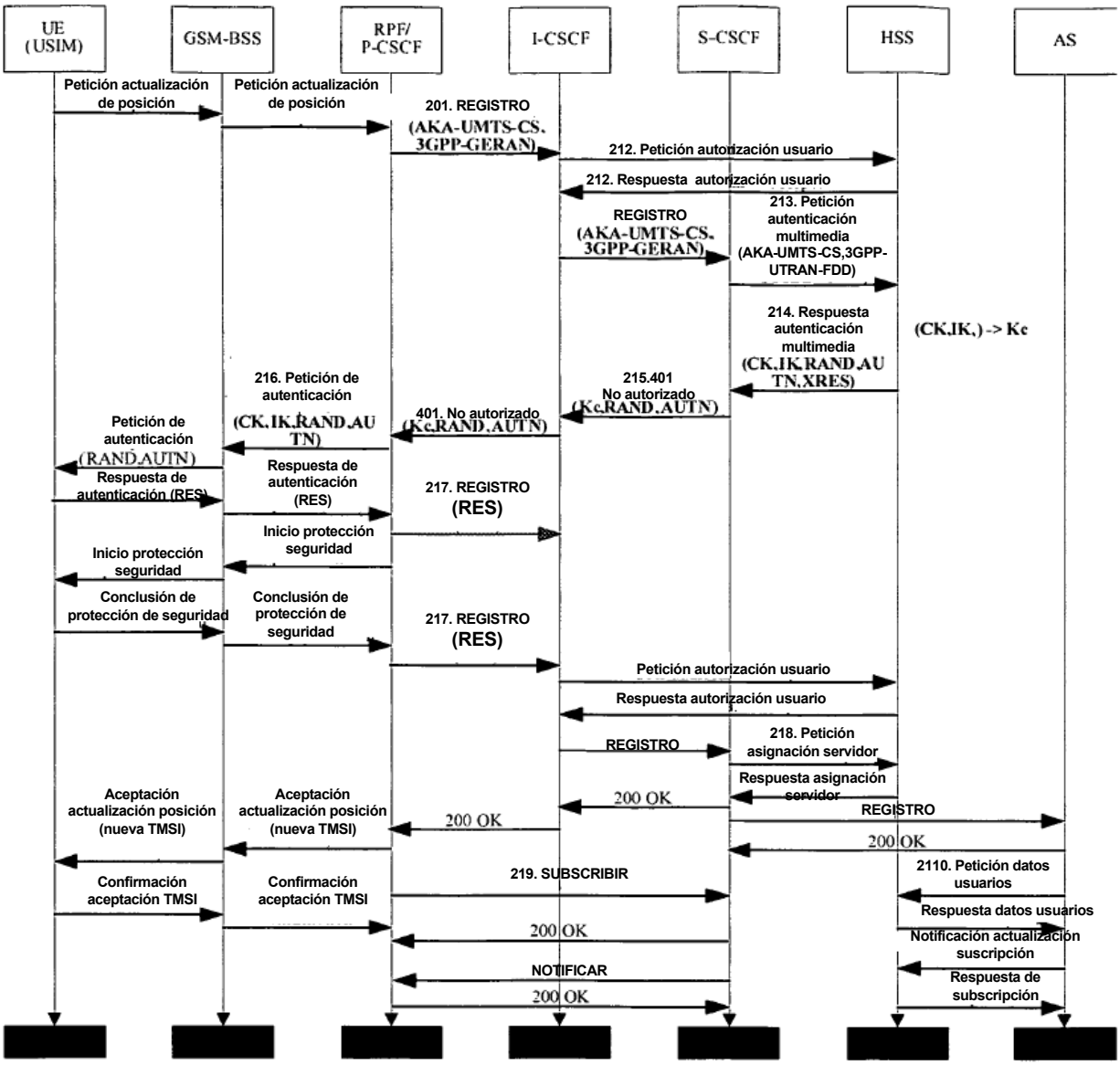

UE (USIM)
RNS
RPF/ P-CSCF
I-CSCF
S-CSCF
HSS
AS
Petición actualización de posición
Petición actualización de posición
201. REGISTRO (AKA-UMTS-CS, 3GPP-UTRAN-FDD)
202. Petición autorización usuario
202. Respuesta autorización usuario
REGISTRO (AKA-UMTS-CS, 3GPP-UTRAN-FDD)
203. Petición autenticación multimedia (AKA-UMTS-CS,3GPP-UTRAN-FDD)
204. Respuesta autenticación multimedia (CK,IK,RAND,AUTN,XRES)
205.401 No autorizado (CK,IK,RAND,AUTN)
401. No autorizado (CK,IK,RAND,AUTN)
06. Petición de autenticación (CK,IK,RAND,AUTN)
Petición de autenticación (RAND,AUTN)
Respuesta de autenticación (RES)
Respuesta de autenticación (RES)
207. REGISTRO (RES)
Inicio protección seguridad
Inicio protección seguridad
Conclusión de protección de seguridad
Conclusión de protección de seguridad
207. REGISTRO (RES)
Petición autorización usuario
Respuesta autorización usuario
208. Petición asignación servidor
208. Respuesta asignación servidor
208.200 OK
208.200 OK
REGISTRO
200 OK
Aceptación actualización posición (nueva TMSI)
Aceptación actualización posición (nueva TMSI)
2010. Petición datos usuarios
209. SUBSCRIBIR
Confirmación aceptación TMSI
Confirmación aceptación TMSI
Respuesta datos usuarios
200 OK
NOTIFICAR
Notificación actualización suscripción
Respuesta de subscripción
200 OK

Figura 19


UE (USIM)
GSM-BSS
RPF/ P-CSCF
I-CSCF
S-CSCF
HSS
AS
Petición actualización de posición
Petición actualización de posición
201. REGISTRO (AKA-UMTS-CS, 3GPP-GERAN)
212. Petición autorización usuario
212. Respuesta autorización usuario
REGISTRO (AKA-UMTS-CS, 3GPP-GERAN)
213. Petición autenticación multimedia (AKA-UMTS-CS,3GPP-UTRAN-FDD)
214. Respuesta autenticación multimedia (CK,IK,RAND,AUTN,XRES)
(CK,IK,) -> Kc
216. Petición de autenticación (CK,IK,RAND,AUTN)
215.401 No autorizado (Kc,RAND,AUTN)
401. No autorizado (Kc,RAND,AUTN)
Petición de autenticación (RAND,AUTN)
Respuesta de autenticación (RES)
Respuesta de autenticación (RES)
217. REGISTRO (RES)
Inicio protección seguridad
Inicio protección seguridad
Conclusión de protección de seguridad
Conclusión de protección de seguridad
217. REGISTRO (RES)
Petición autorización usuario
Respuesta autorización usuario
REGISTRO
218. Petición asignación servidor
Respuesta asignación servidor
200 OK
Aceptación actualización posición (nueva TMSI)
Aceptación actualización posición (nueva TMSI)
200 OK
REGISTRO
200 OK
Confirmación aceptación TMSI
Confirmación aceptación TMSI
219. SUBSCRIBIR
2110. Petición datos usuarios
Respuesta datos usuarios
200 OK
Notificación actualización suscripción
NOTIFICAR
Respuesta de subscripción
200 OK

Pagina 20

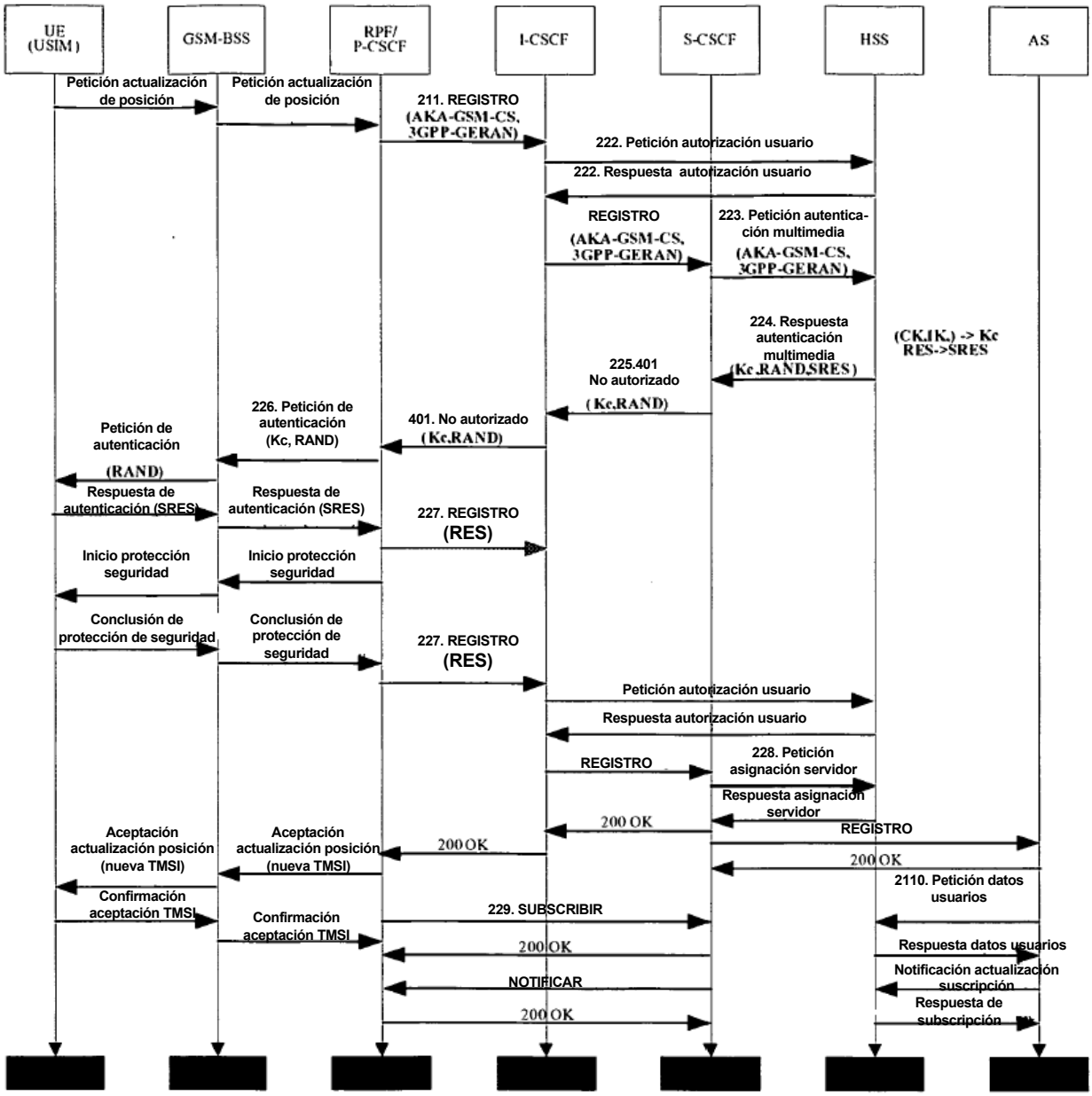

UE (USIM)
GSM-BSS
RPF/ P-CSCF
I-CSCF
S-CSCF
HSS
AS
Petición actualización de posición
Petición actualización de posición
211. REGISTRO (AKA-GSM-CS, 3GPP-GERAN)
222. Petición autorización usuario
222. Respuesta autorización usuario
REGISTRO (AKA-GSM-CS, 3GPP-GERAN)
223. Petición autentica-ción multimedia (AKA-GSM-CS, 3GPP-GERAN)
224. Respuesta autenticación multimedia (Kc,RAND,SRES)
(CK,IK) -> Kc RES->SRES
225.401 No autorizado
(Kc,RAND)
226. Petición de autenticación (Kc, RAND)
401. No autorizado (Kc,RAND)
Petición de autenticación (RAND)
Respuesta de autenticación (SRES)
Respuesta de autenticación (SRES)
227. REGISTRO (RES)
Inicio protección seguridad
Inicio protección seguridad
Conclusión de protección de seguridad
Conclusión de protección de seguridad
227. REGISTRO (RES)
Petición autorización usuario
Respuesta autorización usuario
REGISTRO
228. Petición asignación servidor
Respuesta asignación servidor
200 OK
REGISTRO
Aceptación actualización posición (nueva TMSI)
Aceptación actualización posición (nueva TMSI)
200 OK
200 OK
2110. Petición datos usuarios
Confirmación aceptación TMSI
Confirmación aceptación TMSI
229. SUBSCRIBIR
200 OK
Respuesta datos usuarios
Notificación actualización suscripción
NOTIFICAR
Respuesta de subscripción
200 OK

Figura 21

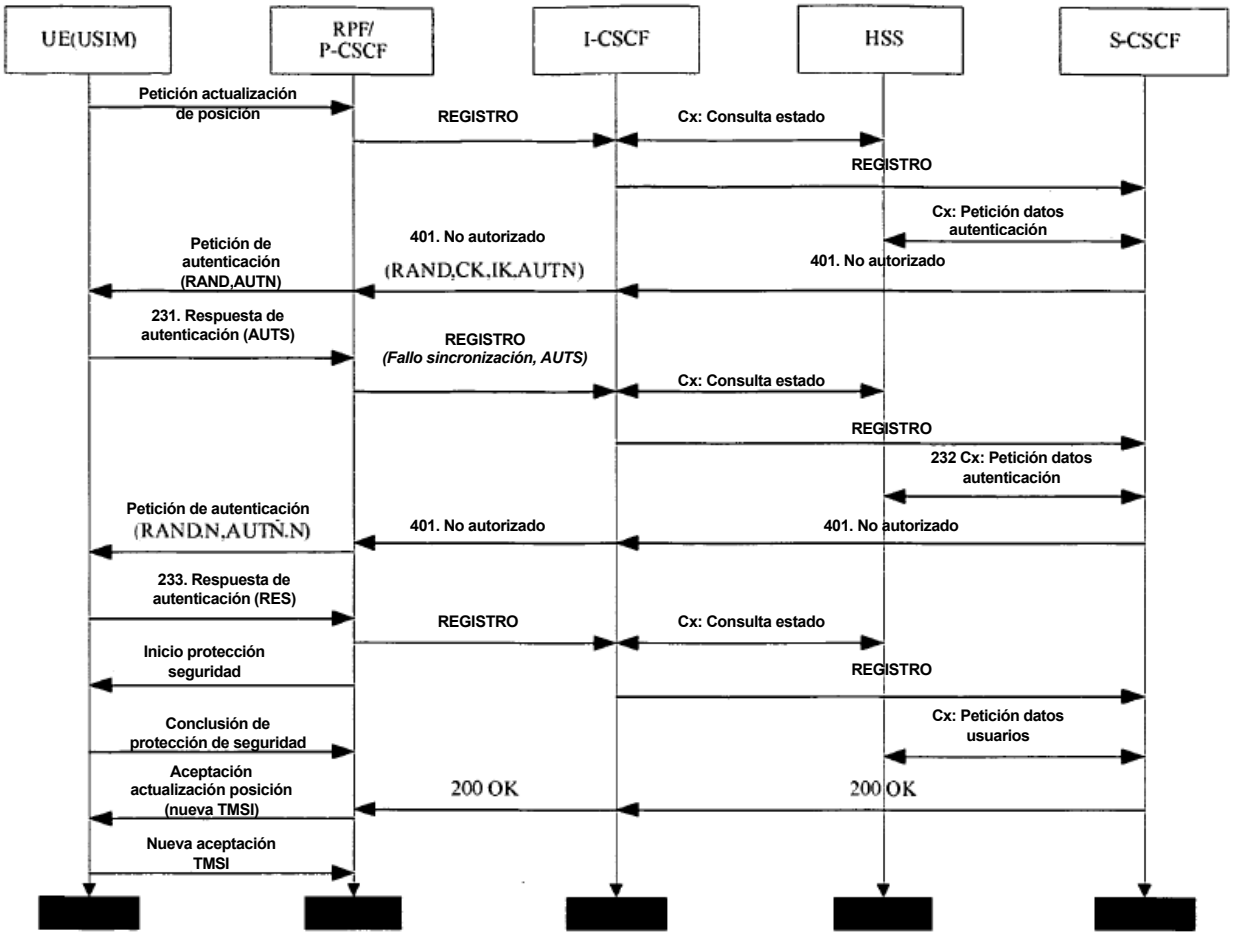

UE(USIM)
RPF/ P-CSCF
I-CSCF
HSS
S-CSCF
Petición actualización de posición
REGISTRO
Cx: Consulta estado
REGISTRO
Cx: Petición datos autenticación
401. No autorizado
(RAND,CK,IK,AUTN)
Petición de autenticación (RAND,AUTN)
401. No autorizado
231. Respuesta de autenticación (AUTS)
REGISTRO
(Fallo sincronización, AUTS)
Cx: Consulta estado
REGISTRO
232 Cx: Petición datos autenticación
Petición de autenticación
(RAND,N,AUTN,N)
401. No autorizado
401. No autorizado
233. Respuesta de autenticación (RES)
REGISTRO
Cx: Consulta estado
Inicio protección seguridad
REGISTRO
Cx: Petición datos usuarios
Conclusión de protección de seguridad
Aceptación actualización posición (nueva TMSI)
200 OK
200 OK
Nueva aceptación TMSI

Figura 22

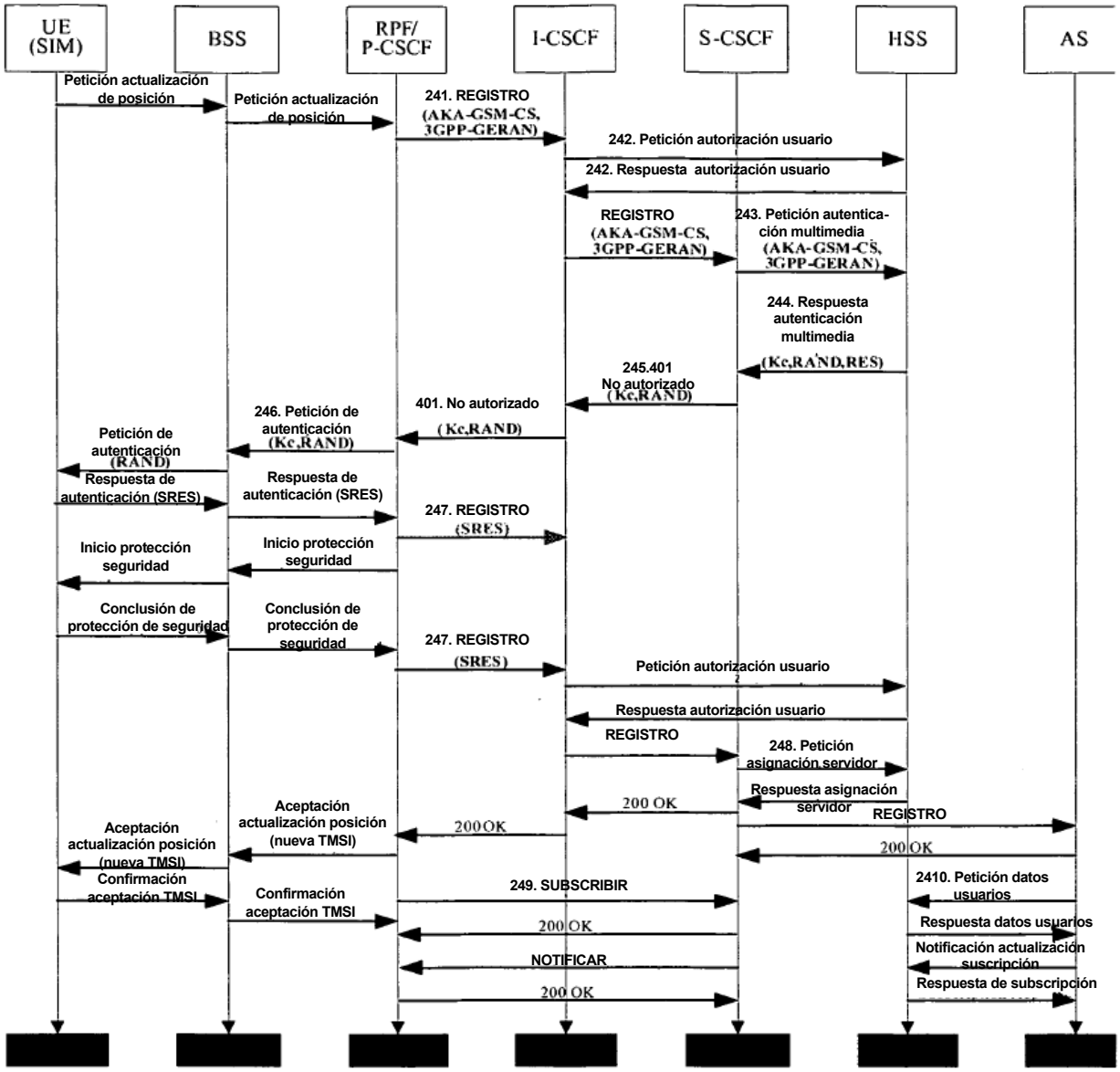

UE (SIM)
BSS
RPF/ P-CSCF
I-CSCF
S-CSCF
HSS
AS
Petición actualización de posición
Petición actualización de posición
241. REGISTRO (AKA-GSM-CS, 3GPP-GERAN)
242. Petición autorización usuario
242. Respuesta autorización usuario
REGISTRO (AKA-GSM-CS, 3GPP-GERAN)
243. Petición autentica-ción multimedia (AKA-GSM-CS, 3GPP-GERAN)
244. Respuesta autenticación multimedia (Kc,RAND,RES)
245.401 No autorizado (Kc,RAND)
401. No autorizado (Kc,RAND)
246. Petición de autenticación (Kc,RAND)
Petición de autenticación (RAND)
Respuesta de autenticación (SRES)
Respuesta de autenticación (SRES)
247. REGISTRO (SRES)
Inicio protección seguridad
Inicio protección seguridad
Conclusión de protección de seguridad
Conclusión de protección de seguridad
247. REGISTRO (SRES)
Petición autorización usuario
Respuesta autorización usuario
REGISTRO
248. Petición asignación servidor
Respuesta asignación servidor
200 OK
REGISTRO
Aceptación actualización posición (nueva TMSI)
200 OK
Aceptación actualización posición (nueva TMSI)
200 OK
Confirmación aceptación TMSI
249. SUBSCRIBIR
2410. Petición datos usuarios
Confirmación aceptación TMSI
Respuesta datos usuarios
200 OK
Notificación actualización suscripción
NOTIFICAR
Respuesta de subscripción
200 OK

Figura 23

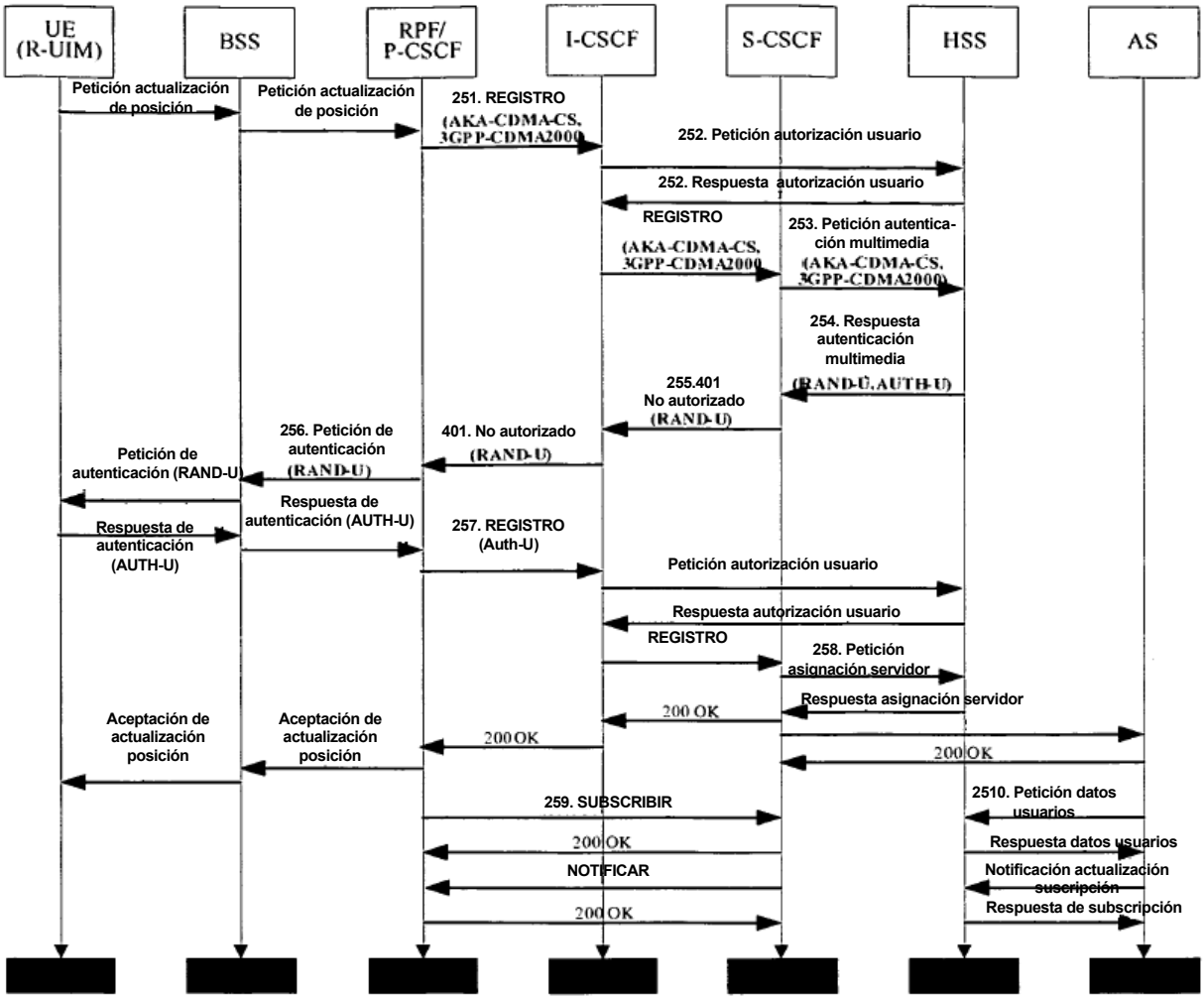


Figura 24

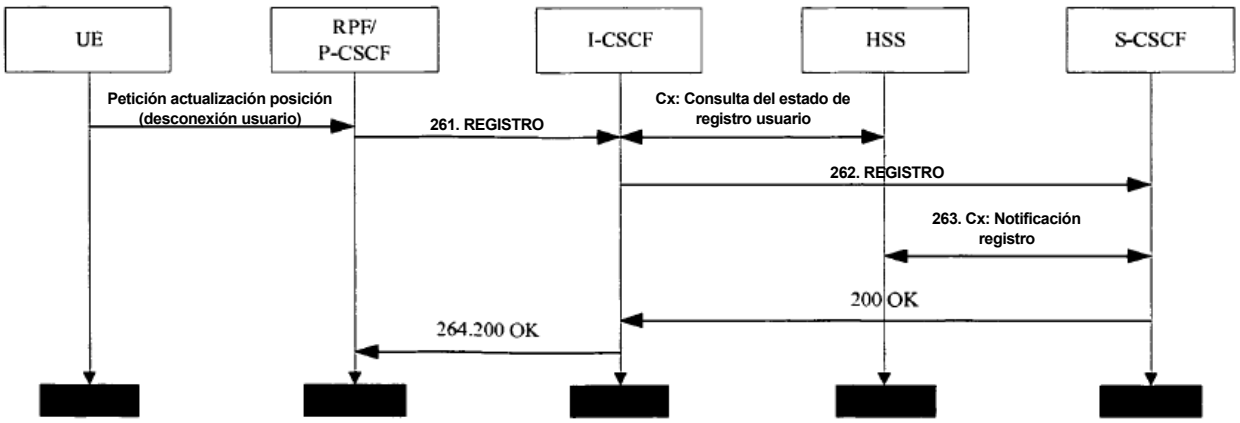


Figura 25