(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 645 270**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.08.2003 E 13172208 (4)**

(97) Fecha y número de publicación de la concesión europea: **26.07.2017 EP 2642723**

(54) Título: **Aparato y método para autenticar a un usuario cuando accede a servicios multimedia**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.12.2017

(73) Titular/es:

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

(72) Inventor/es:

WALKER PINA, JOHN MICHAEL y
SANCHEZ HERRERO, JUAN ANTONIO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Aparato y método para autenticar a un usuario cuando accede a servicios multimedia

Campo de la invención

La presente invención se refiere a un procedimiento simplificado para la autenticación de un usuario que accede a una red multimedia a través de una red de acceso en la que el usuario ya había sido autenticado.

Antecedentes

Muchas de las redes móviles actualmente existentes, así como posibles redes futuras definidas por los cuerpos de normalización, necesitan la autenticación de los usuarios finales y de los agentes de usuario cuando acceden a una red y, más bien, cuando acceden a servicios asociados a la red. A este respecto, los dominios de GSM, GPRS, la red de área local inalámbrica (WLAN – Wireless Local Area Network, en inglés) y multimedia (IMS) tal como están definidos por los estándares 3GPP y 3GPP2, necesitan, todos ellos, la ejecución por parte del equipo o los terminales de usuario de un procedimiento de autenticación específico para cada dominio tecnológico particular antes de conceder a los usuarios o a los agentes de usuarios el acceso a dichos dominios. En particular, los dominios tecnológicos citados anteriormente, así como otros dominios tecnológicos emergentes, requieren diferentes niveles de seguridad que complican más el acceso a través de los diferentes dominios tecnológicos. Este acceso implica una seguridad adicional que no siempre es necesaria y, como consecuencia, un procesamiento adicional y capacidades de señalización, así como una complejidad extra en el equipo o los terminales del usuario.

En la actualidad, el procedimiento de autenticación en un dominio multimedia 3GPP se lleva a cabo tal como se describe en el estándar 3GPP TS 33.203 V5.6.0 y está representado en la figura 1 en términos de un Flujo de señalización basado en el protocolo de inicio de sesión (SIP – Session Initiation Protocol, en inglés). Como muestra la figura 1 y describen las memorias descriptivas referidas, la autenticación multimedia se llevará a cabo siempre cuando un usuario se registra en el dominio multimedia, lo que inicia típicamente enviando un mensaje de inicio de sesión de SIP para una identidad privada y pública dada.

Una condición inicial supuesta antes de inicial el flujo citado anteriormente es que un usuario final debe tener una conexión de datos abierta antes de acceder al dominio multimedia. Esta conexión puede ser una conexión GPRS en términos de tener un contexto de PDP activado, o una conexión WLAN en términos de haber establecido una conexión de datos tal como se especifica mediante los estándares IEEE 802.11, u otra red de acceso que proporciona al lado de usuario una conexión de datos. En este escenario, un usuario final o un agente de usuario ha sido ya autenticado por la red de acceso, ya sea el GPRS, o la WLAN u otro, con el fin de establecer dicha conexión de datos y antes de enviar un inicio de sesión de SIP al dominio multimedia.

En particular, ambas redes de acceso actualmente utilizadas, a saber, GPRS y WLAN, están ofreciendo un mecanismo de autenticación respectivo, SIM/USIM-AKA para GPRS y EAP SIM/AKA para WLAN, mientras que el dominio multimedia utiliza actualmente un mecanismo de autenticación que ofrece un nivel de seguridad similar al de las redes de acceso anteriores, el denominado USIM-AKA, que se lleva a cabo cuando el mensaje de inicio de sesión de SIP llega a una entidad de función de control de estado de llamada de servicio (S-CSCF – Serving Call Status Control Function, en inglés) tal como se muestra en la figura 1. A este respecto, la figura 2 muestra la secuencia de acciones seguidas para llevar a cabo una autenticación AKA de EAP para un usuario que ha accedido a una red WLAN en la que RADIUS y MAP parecen ser las alternativas de protocolo más probables, aunque también se podría utilizar DIAMETER en lugar de RADIUS o MAP.

En la actualidad, un usuario que desea acceder al dominio multimedia requiere un establecimiento previo de una conexión de datos, lo que frecuentemente se realiza a través de una red de acceso tal como GPRS o WLAN y, por consiguiente, el usuario ha sido autenticado en primer lugar con un EAP-SIM/AKA para una red de acceso WLAN y, además, el usuario debe ser autenticado en segundo lugar con un USIM-AKA cuando se registra en el dominio multimedia.

Se puede concluir que actualmente no existe ningún mecanismo de autenticación que realice una autenticación entre dominios para un usuario dado entre una red de acceso tal como GPRS o WLAN y un dominio multimedia basado en SIP. En otras palabras, no existe ningún servicio o dispositivo que sea capaz de administrar datos de autenticación en nombre de un usuario o un agente de usuario de SIP y de liberar dicho usuario o agente de usuario de SIP de tener que realizar operaciones de autenticación en el dominio multimedia una vez que una autenticación ya ha tenido lugar en la red de acceso a través de la que el usuario accede, siendo dicha red de acceso probablemente GPRS o WLAN.

En esta situación, la autenticación para el dominio multimedia tal como se describe en el documento 3G TS 33.203 y se muestra en la figura 1 añade señalización adicional en la ruta de radio que, en algunos escenarios, podría ser innecesaria. En primer lugar, después de que la S-SCSF recibe un inicio de sesión de SIP, la S-SCSF normalmente envía un mensaje de pregunta de autenticación al agente de usuario de SIP. Si esta operación tiene éxito, entonces la S-CSCF enviará periódicamente una solicitud de vector de autenticación al agente de usuario de SIP que, a su vez, debe responder con una respuesta de vector de autenticación. Ambos mensajes añaden carga adicional en el

dominio multimedia, así como tiempos más largos de inicio de sesión. Es decir, los agentes de usuario de SIP deben procesar y responder tanto a la pregunta de autenticación como a la solicitud de vector de autenticación. Estos mensajes requieren un procesamiento adicional por el agente de usuario de SIP, lo que significa que el agente de usuario de SIP tiene que utilizar la energía para este proceso en lugar de utilizar la mayor cantidad de energía posible para los servicios de multimedia que probablemente son de alto consumo de energía, y teniendo en cuenta el poder limitado de las baterías.

De este modo, la presente invención tiene por objeto proporcionar un mecanismo de autenticación entre dominios que realice una autenticación entre dominios para un usuario dado entre un dominio de la red de acceso y un dominio multimedia, siendo este mecanismo de autenticación entre dominios más simple que el existente actualmente, y aplicable cuando ha sido realizada una autenticación de usuario por la red de acceso.

Compendio de la invención

El objetivo anterior se lleva a cabo de acuerdo con la presente invención mediante la utilización del equipo de usuario de la reivindicación 1, el método de la reivindicación 10 y el sistema de la reivindicación 19.

Se pueden disponer realizaciones para reutilizar datos de autenticación entre diferentes redes o entre diferentes dominios tecnológicos y, con ayuda de un dispositivo para la autenticación de multimedia de un usuario (UE), una entidad de servicio encargada de autenticar al usuario en el dominio multimedia, y de una entidad de Proxy y una entidad de interrogación, estando ambas entidades de un dominio multimedia de acuerdo con las normas 3GPP y 3GPP2. Por lo tanto, existe una nueva característica proporcionada de acuerdo con la invención y denominada en lo sucesivo "autenticación implícita para dominio multimedia", que puede ser implementada como un dispositivo de autenticación multimedia exclusivo en estrecha cooperación con un servidor de abonado, o puede estar totalmente integrado en dicho servidor de abonado. Siendo dicho servidor de abonado una base de datos de abonados implicada durante la autenticación de abonado, por ejemplo, un servidor de abonado doméstico (HSS – Home Subscriber Server, en inglés) o un servidor de autenticación-autorización-contabilidad (AAA – Authentication – Authorisation – Accounting, en inglés) y el dispositivo de autenticación multimedia que contiene la lógica y los componentes necesarios para permitir la reutilización de datos de autenticación entre una red de acceso, tal como una red de área local inalámbrica (WLAN – Wireless Local Area Network, en inglés), una red de sistema general de radio de paquetes (GPRS – General Packet Radio System, en inglés), un sistema universal de telecomunicaciones móviles (UMTS – Universal Mobile Telecommunications System, en inglés) o una red de acceso múltiple por división de código (CDMA 2000 – Code Division Multiple Access 2000, en inglés) y dicho dominio multimedia.

Según un primer aspecto de la invención, se proporciona un equipo de usuario (UE – User Equipment, en inglés) capacitado para obtener acceso al dominio multimedia (IMS) a través de una red de acceso, dispuesta para llevar a cabo un procedimiento de autenticación explícito con la red de acceso, y dispuesta para realizar posteriormente un procedimiento de autenticación implícito con el dominio multimedia (IMS). Este equipo de usuario (UE) puede estar dispuesto para enviar un mensaje de inicio de sesión que indica que se propone una autenticación implícita del equipo de usuario (UE) hacia el dominio multimedia (IMS).

De acuerdo con un segundo aspecto de la invención, se proporciona un método para que un equipo de usuario (UE) obtenga acceso a un dominio multimedia (IMS) a través de una red de acceso, comprendiendo el método: el equipo de usuario (UE) lleva a cabo un procedimiento de autenticación explícito con la red de acceso; y el equipo de usuario (UE) lleva a cabo posteriormente un procedimiento de autenticación implícito con el dominio multimedia (IMS).

De acuerdo con un tercer aspecto de la invención, se proporciona un sistema para proporcionar un acceso de equipo de usuario (UE) a un dominio multimedia (IMS) a través de una red de acceso, comprendiendo el sistema el dominio multimedia (IMS), la red de acceso y el equipo de usuario (UE) según cualquiera de las reivindicaciones 1 a 10.

Un dispositivo, que de acuerdo con la invención es útil para la autenticación multimedia de un usuario que accede a un dominio multimedia a través de una red de acceso, está dispuesto para su uso en, o en cooperación con, un servidor de abonado de la red de acceso que contiene datos de autenticación para usuario y es accesible al dominio multimedia. Dicho dispositivo comprende un medio para decidir que puede tener lugar una autenticación implícita entre el usuario o, más bien, entre el equipo de usuario y el dominio multimedia, y medios para dar instrucciones a una entidad de servicio encargada de autenticar al usuario en el dominio multimedia de que la autenticación implícita puede tener lugar la utilización de este dispositivo evitando de este modo la necesidad de una autenticación explícita.

En este dispositivo, el medio para decidir que puede tener lugar una autenticación implícita incluye preferiblemente un medio para determinar la seguridad potencial de la ruta de señalización para acceder al dominio multimedia a través de dicha red de acceso. Para ello, el dispositivo puede comprender asimismo un medio de aprovisionamiento y configuración de datos dispuesto para evaluar la seguridad de diferentes rutas de señalización. Además, el medio para decidir que puede tener lugar una autenticación implícita puede incluir un medio para procesar una propuesta de autenticación implícita originada en el equipo de usuario.

El dispositivo está dispuesto ventajosamente para determinar si una autenticación implícita es solo una propuesta al equipo de usuario, que puede forzar una autenticación explícita, o es una decisión final adoptada por la red, de modo que no se puede realizar una autenticación explícita. Por lo tanto, los medios para dar instrucciones a la entidad de servicio que pueden implicar una autenticación implícita incluyen medios para indicar que la decisión final está en el equipo de usuario y medios para indicar que se trata de una decisión final adoptada por la red.

A este respecto, el dispositivo comprende además un medio para notificar al usuario que una autenticación implícita del usuario para acceder al dominio multimedia puede ser llevada a cabo por la red. Sin embargo, este medio de notificación podría residir asimismo en otras entidades del dominio multimedia.

Además, dado que la decisión final sobre si realizar o no una autenticación implícita puede estar en el lado del equipo de usuario de acuerdo con la invención, el dispositivo comprende además medios para recibir una indicación originada desde el lado del equipo de usuario para confirmar la aceptación de la autenticación implícita propuesta por la red. En el caso de recibir dicha confirmación de aceptación, el dispositivo comprende asimismo medios para indicar a la entidad de servicio encargada de autenticar al usuario en el dominio multimedia que el equipo de usuario ha confirmado la autenticación implícita. Más aún, el dispositivo puede tener los medios para proporcionar datos de autenticación adicionales a dicha entidad de servicio, incluyendo dichos datos de autenticación adicionales al menos un elemento seleccionado de un grupo de elementos que comprende: tipo de autenticación, información de acceso y marca de tiempo de autenticación.

Convencionalmente, un equipo de usuario está capacitado para obtener acceso a un dominio multimedia a través de una red de acceso, y por lo tanto está dispuesto para llevar a cabo un primer procedimiento de autenticación explícita con la red de acceso, y un segundo procedimiento de autenticación explícita con un dominio multimedia. La red de acceso comprende un servidor de abonado para contener datos de autenticación para el usuario y, para el propósito de la presente invención, dicho servidor de abonado es accesible al dominio multimedia. El equipo de usuario, de acuerdo con la invención, comprende medios para procesar al menos una notificación seleccionada de un grupo de notificaciones que incluyen: una notificación desde el dominio multimedia indicando que se puede llevar a cabo una autenticación implícita para el usuario; y una notificación hacia el dominio multimedia indicando que el equipo de usuario propone una autentificación implícita a la red.

Estos medios pueden incluir ventajosamente medios para recibir una indicación desde el dominio multimedia de que la decisión final está en el lado del equipo de usuario, que podría forzar una autenticación explícita, o que es una decisión final adoptada por la red, de modo que no se pueda realizar ninguna autentificación explícita. Especialmente dispuesto para el caso de que la decisión final esté en el lado del usuario, el equipo de usuario comprende medios para enviar hacia el dominio multimedia una indicación para confirmar la aceptación de una autenticación implícita propuesta por la red. Además, el equipo de usuario puede tener los medios para proporcionar datos de autenticación adicionales al dominio multimedia, comprendiendo dichos datos de autenticación adicionales al menos un elemento seleccionado de un grupo de elementos que comprende: tipo de autenticación; información de acceso; y marca de tiempo de autenticación.

Asimismo, se proporciona un método para autenticar un usuario en un dominio multimedia cuando el usuario accede a él a través de una red de acceso, comprendiendo el método convencionalmente una etapa de autenticación del usuario en la red de acceso, teniendo dicha red de acceso un servidor de abonado con datos de autenticación para el usuario y accesibles al dominio multimedia; y una etapa de registrar al usuario en el dominio multimedia.

Este método, de acuerdo con la invención comprende, asimismo: una etapa de decidor que puede tener lugar una autentificación implícita entre el usuario y el dominio multimedia, evitando de este modo las necesidades de una autenticación explícita; y una etapa de dar instrucciones a una entidad de servicio encargada de autenticar al usuario en el dominio multimedia de que puede tener lugar la autentificación implícita.

Este método puede comprender además una etapa de notificación desde el dominio multimedia al equipo de usuario que se puede llevar a cabo una autenticación implícita del usuario para acceder al dominio multimedia.

En este método, la etapa de decidir que una autenticación implícita puede tener lugar preferiblemente incluye una etapa de determinar la seguridad potencial de la ruta de señalización para acceder al dominio multimedia a través de dicha red de acceso. Además, la etapa anterior de decidir que puede tener lugar una autenticación implícita puede incluir asimismo una etapa de proponer desde el equipo de usuario hacia el dominio multimedia la realización de una autenticación implícita entre el equipo de dicho usuario y el dominio multimedia.

También en este método, la etapa de dar instrucciones a la entidad de servicio de que puede tener lugar una autenticación implícita incluye preferiblemente una etapa de indicar si la decisión final está en el equipo de usuario, lo que podría forzar una autenticación explícita, o la decisión está adoptada por la red, de tal manera que no es posible realizar una autenticación explícita. Además, y, específicamente para el caso en que la decisión final está del lado del usuario, el método puede comprender asimismo una etapa de confirmación desde el equipo de usuario de la aceptación de la autenticación implícita propuesta por la red. Además, y alineado con la etapa anterior, el método puede comprender asimismo una etapa de indicar a la entidad de servicio encargada de autenticar al usuario en el dominio multimedia que el usuario ha confirmado la autenticación implícita.

La invención proporciona asimismo una entidad de servicio encargada de autenticar el equipo de un usuario en el dominio multimedia cuando el usuario accede a él a través de una red de acceso en la que dicho usuario había sido previamente autenticado. Esta entidad de servicio comprende, de acuerdo con la invención, medios para recibir instrucciones del dispositivo anterior indicando que puede tener lugar una autenticación implícita; y un medio para notificar al equipo de usuario que una autenticación implícita del usuario para acceder al dominio multimedia puede ser llevada a cabo por la red.

Esta entidad de servicio está ventajosamente dispuesta de tal manera que el medio para notificar al usuario que una autenticación implícita puede ser llevada a cabo por la red incluye medios para indicar al usuario si la autenticación implícita es una decisión final adoptada por la red y no se puede llevar a cabo ninguna autenticación explícita, o la autenticación implícita es una propuesta de la red que el usuario puede aceptar o rechazar obligando a una autenticación explícita.

En el caso de que la autenticación implícita sea una propuesta de la red, la entidad de servicio comprende ventajosamente medios para recibir una indicación originada desde el equipo de usuario para confirmar la aceptación de dicha autenticación implícita propuesta por la red. Además, esta entidad de servicio comprende preferiblemente medios para recibir dicha indicación de que el usuario ha confirmado la autenticación implícita del dispositivo anterior.

Esta entidad de servicio puede comprender ventajosamente otros medios para comprobar la coincidencia de datos de autenticación adicionales recibidos respectivamente del dispositivo y del equipo de usuario anteriores con el fin de proporcionar un soporte de seguridad adicional. Estos datos de autenticación adicionales incluyen al menos un elemento de un grupo de elementos que comprende: tipo de autenticación, información de acceso y marca de tiempo de autenticación.

La invención se complementa adicionalmente con la provisión de algunas otras entidades, tales como un servidor de proximidad y una entidad de interrogación, con el fin de abordar una topología típica siguiendo un estándar 3GPP o un estándar 3GPP2.

La entidad de servidor de proximidad, de acuerdo con los estándares 3GPP y 3GPP2, está destinada a actuar como punto de entrada en el dominio multimedia para los usuarios que acceden a él a través de una red de acceso, donde el usuario ya había sido autenticado. Esta entidad servidor de proximidad, de acuerdo con la invención, comprende medios para procesar al menos una notificación seleccionada de un grupo de notificaciones que incluye: una notificación enviada hacia el equipo de usuario para indicar que una autenticación implícita del usuario para acceder al dominio multimedia puede ser llevada a cabo fuera de la red; y una notificación recibida del equipo de usuario para proponer una autentificación implícita hacia el dominio multimedia entre dicho equipo de usuario y el dominio multimedia.

Esta entidad de servidor de proximidad está ventajosamente dispuesta asimismo de tal manera que el medio para notificar al usuario que una autenticación implícita puede ser llevada a cabo por la red incluye medios para indicar al usuario si la autenticación implícita es una decisión final adoptada por la red y no se puede llevar a cabo ninguna autenticación explícita, o la autenticación implícita es una propuesta de la red que el usuario puede aceptar o rechazar forzando una autenticación explícita.

En el caso de que la autenticación implícita sea una propuesta de la red, la entidad servidor de proximidad ventajosamente comprende medios para recibir una indicación desde el equipo de usuario de que acepta dicha autenticación implícita propuesta por la red.

La entidad de interrogación, de acuerdo con los estándares 3GPP y 3GPP2, tiene la intención de consultar a un servidor de abonado en el dominio multimedia acerca de un usuario que ha accedido a dicho dominio multimedia a través de otra red de acceso. Esta entidad de interrogación tiene medios para recibir una solicitud de inicio de sesión del usuario, y medios para reconocer tal inicio de sesión hacia el usuario y, de acuerdo con la invención, la entidad de interrogación comprende asimismo medios para transmitir una indicación hacia el equipo de usuario de que se puede llevar a cabo una autenticación implícita del usuario para acceder al dominio multimedia.

La entidad de interrogación, con el fin de conseguir otras características ventajosas proporcionadas por la invención, comprende preferiblemente medios para recibir una indicación originada desde el equipo de usuario para confirmar la aceptación de una autenticación implícita propuesta por la red o para proponer tal autenticación implícita por sí mismo; y medios para transmitir dicha confirmación de aceptación del usuario hacia al menos una entidad seleccionada de un grupo de entidades que comprenden el dispositivo anterior y la entidad de servicio.

Además, y también para conseguir otras características ventajosas proporcionadas por la invención, la entidad de interrogación comprende además medios para transmitir hacia el equipo de usuario una indicación de que la autenticación implícita es una decisión final adoptada por la red y que no se puede realizar ninguna autenticación explícita.

Breve descripción de los dibujos

Las características, objetos y ventajas de la invención se harán evidentes mediante la lectura de esta descripción conjuntamente con los dibujos adjuntos, en los cuales:

La figura 1 muestra un diagrama básico del flujo de autenticación en un dominio multimedia de acuerdo con el documento 3GPP TS 33.203.

La figura 2 muestra una vista general de los componentes de la disposición y el flujo de señalización durante la autenticación de un usuario mediante un mecanismo de EAP-AKA a través de una red de acceso WLAN.

La figura 3 muestra una secuencia de flujo que describe una realización actualmente preferida para reutilizar la autenticación previa de un usuario que ha accedido a través de una red GPRS o UMTS al dominio multimedia, donde el equipo de usuario recibe una notificación a este respecto y se le da la posibilidad de aceptar o no una autenticación implícita.

La figura 4 muestra una secuencia de flujo que describe una realización alternativa a la mostrada en la figura 3, en la que el equipo de usuario recibe una notificación a este respecto y sin que se le dé la posibilidad de aceptar o no una autenticación implícita, sino que más bien se le informa de que dicha autenticación implícita ha tenido lugar.

La figura 5 muestra una secuencia de flujo alternativa que describe una realización alternativa a las mostradas en la figura 3 y la figura 4, donde el equipo de usuario recibe una invitación durante el procedimiento de localización para llevar a cabo una autenticación implícita hacia el dominio multimedia, teniendo de este modo el usuario la posibilidad de aceptar o no una autenticación implícita.

La figura 6 muestra una secuencia de flujo alternativa a la mostrada en la Figura 5, en la que el equipo de usuario recibe una invitación con un servicio de mensajes cortos (SMS – Short Message Service, en inglés) para llevar a cabo una autenticación implícita hacia el dominio multimedia, teniendo el usuario, por lo tanto, la posibilidad de aceptar o no una autenticación implícita.

La figura 7 muestra una secuencia de flujo que describe una realización actualmente preferida para reutilizar la autenticación previa de un usuario que tiene acceso a través de una red WLAN al dominio multimedia, donde el equipo de usuario recibe una notificación a este respecto y se le da la posibilidad de aceptar o no una autenticación implícita.

La figura 8 muestra una secuencia de flujo que describe otra realización preferida para reutilizar la autenticación previa de un usuario mediante una red CDMA 2000, accediendo el usuario a través de una red de servicios de paquetes de datos al dominio multimedia donde el equipo de usuario recibe una notificación a este respecto y se le da la posibilidad de aceptar o no una autenticación implícita.

La figura 9 muestra una secuencia de flujo alternativa a las presentadas en las figuras 5 y 6, en la que el equipo de usuario no recibe una invitación, con un mensaje de respuesta de actualización de localización o con un servicio de mensajes cortos (SMS) respectivamente para llevar a cabo una autenticación implícita pero, más bien, el equipo de usuario genera una propuesta para una autentificación implícita a la red.

Descripción de realizaciones preferidas

A continuación, se describen realizaciones actualmente preferidas de: un aparato, un equipo de usuario y un método para ofrecer a un usuario la posibilidad de ser implícitamente autenticado por un dominio multimedia cuando accede a través de una red de acceso en la que el usuario ya ha sido autenticado. Preferiblemente, la red de acceso es una red de área local inalámbrica (WLAN), una red del sistema general de radiocomunicaciones en paquetes (GPRS), una red del sistema global para comunicaciones móviles (GSM – Global System for Mobile communications, en inglés), o una red del sistema universal de telecomunicación móvil (UMTS - Universal Mobile Telecommunication System, en inglés) o una red de acceso múltiple por división de código (CDMA 2000).

La presente invención presenta varias realizaciones en relación con el lugar en el que reside la característica "autenticación implícita para dominio multimedia", que, en particular, pueden llevarse a cabo mediante un dispositivo aislado en estrecha cooperación con un servidor de abonado o ser transportado por el propio servidor de abonado.

Además, la presente invención presenta asimismo varias realizaciones relacionadas con el equipo de usuario, es decir, el terminal del usuario, o SIM, o USIM, o combinaciones de los mismos, dependiendo del grado de decisión que queda en el lado del usuario o en el lado de la red.

De acuerdo con una realización de la presente invención, el propio servidor de abonado, que en particular puede ser un HSS en el 3GPP o un servidor AAA en el estándar 3GPP2 y las redes CDMA 2000, o un dispositivo de autenticación multimedia que soporta el acceso al dominio multimedia para un usuario específico determina que puede ser innecesaria una autenticación explícita para el dominio multimedia en base a una autenticación de abonado anterior llevada a cabo por la red de acceso a la que accede el usuario, y en base a la suposición de que se transporta un portador seguro para la señalización multimedia a través de la red de acceso. Dicho portador

seguro puede ser, por ejemplo, un contexto PDP, en el caso de que el GPRS sea la red de acceso o un túnel seguro en el caso de que la WLAN sea la red de acceso hacia la red doméstica mientras se lleva a cabo la autenticación del abonado.

De acuerdo con la invención, el servidor de abonado o el dispositivo de autenticación multimedia exclusivo, proporcionan a una entidad de servicio encargada de autenticar al usuario, a saber, una función de control de estado de llamada de servicio (S-CSCF), una política de autenticación que indica que se puede realizar un procedimiento de autenticación implícito para que dicho usuario acceda al dominio multimedia, en base a una autenticación anterior del portador a través de la red de acceso.

Aparte de la autenticación de un usuario por la red a la que el usuario accede, los procedimientos de autenticación 3GPP admiten la autenticación de la red por parte del usuario. Por lo tanto, de acuerdo con otra realización de la invención, el servidor de abonado o el dispositivo de autenticación multimedia exclusivo pueden, opcionalmente, indicar al equipo de usuario otra política de autenticación para sugerir una posible autenticación implícita mutua que el usuario puede o no aceptar.

Gracias a la característica “autenticación implícita para el dominio multimedia”, se reduce la cantidad de operaciones de autenticación realizadas por el usuario o por el equipo de usuario y por la red y, por lo tanto, se consigue una reducción de mensajes de señalización evitables en el dominio multimedia manteniendo el nivel de seguridad requerido, logrando un objetivo de la presente invención.

La invención es aplicable a diferentes escenarios en los que un usuario hace uso de una red de acceso particular para acceder al dominio multimedia, dando como resultado, por tanto, diferentes realizaciones de la invención. Además, se pueden introducir diversas variaciones de una realización a otra sin apartarse sustancialmente del alcance de la presente invención.

Un primer escenario aparece cuando un usuario ha sido autenticado por una red UMTS y accede además al dominio multimedia a través de una red GPRS.

Bajo este escenario y de acuerdo con una primera realización de la presente invención mostrada en la figura 3, se proporciona un mecanismo simplificado para autenticar al usuario en el dominio multimedia en el que se notifica al usuario una posible autenticación implícita. El usuario, o más bien, el equipo de usuario (UE), tras recibir esta notificación, puede aceptar la autenticación implícita o forzar una autenticación explícita de acuerdo con la norma aplicable para el dominio multimedia, tal como muestra la figura 1. Además, esta autenticación implícita puede aplicarse tanto a la autenticación del usuario por la red como a la autenticación de la red por el usuario. Además, dicha autentificación implícita puede ser activada por un servidor de abonado tal como el servidor de abonado doméstico (HSS) responsable de la autenticación previa del usuario en la red UMTS, tal como se muestra en la Figura 3, o por un dispositivo de autenticación multimedia exclusivo en cooperación con dicho servidor de abonado.

Por lo tanto, de acuerdo con esta primera realización mostrada en la Figura 3, un usuario final o un equipo de usuario final está conectado y autenticado en UMTS y tiene un contexto de PDP de GPRS abierto. En esta etapa, el usuario final y el agente de usuario acceden al dominio multimedia iniciando un procedimiento de inicio de sesión de SIP.

Este procedimiento de inicio de sesión de SIP comprende el envío de un mensaje de inicio de sesión de SIP desde el lado del usuario (UE) hacia una función de control de estado de la llamada del servidor de proximidad (P-CSCF – Proxy Call Status Control Function, en inglés), y desde esta entidad hacia una función de control de estado de la llamada de interrogación (I-CSCF – Interrogating Call Status Control Function). La I-CSCF inicia un procedimiento denominado convencionalmente Cx-Selección-Info hacia el servidor de abonados domésticos (HSS) para identificar la función de control del estado de la llamada de servicio (S-CSCF – Serving Call Status Control Function, en inglés) actualmente a cargo del usuario. Una vez identificada dicha S-CSCF, la I-CSCF envía un mensaje de inicio de sesión de SIP correspondiente a la S-CSCF. La S-CSCF que recibe dicho mensaje de inicio de sesión inicia un procedimiento denominado convencionalmente Cx-Put hacia el servidor de abonados domésticos (HSS).

Dado que el HSS había participado previamente en la autenticación de acceso de GPRS del usuario mediante el intercambio de un perfil de usuario y vectores de autenticación con un nodo de soporte de GPRS de servicio (SGSN – Serving GPRS Support Node, en inglés), el HSS utiliza su información sobre el SGSN en el que está situado el abonado, además de otra información de topología de la red, para determinar la seguridad potencial de la ruta de señalización para acceder al dominio multimedia a través de dicha red de acceso. Por ello, de acuerdo con la invención, el propio HSS, o un dispositivo exclusivo de autenticación multimedia, puede decidir una autenticación implícita para el usuario. Con este fin, el HSS incluye una indicación de autenticación implícita "en la respuesta de Cx-Put a la S-CSCF.

La decisión para enviar este mensaje hacia la S-CSCF se adopta ventajosamente cuando el nodo de soporte de GPRS de la puerta de enlace (GGSN – Gateway GPRS Support Node, en inglés) pertenece al mismo dominio que el HSS y el GGSN es considerado, por lo tanto, seguro y fiable. Un escenario adecuado particular es cuando el HSS también confía en el SGSN en el que está situado el abonado dado que ambos pertenecen a un mismo operador de

la red, por ejemplo, e independientemente de si al usuario se le ha dado o no la posibilidad de rechazar además la autenticación implícita propuesta.

Además, la característica "autenticación implícita para el dominio multimedia" puede incluir el aprovisionamiento de datos y la configuración de datos por abonado de forma que cuando un usuario tiene contratado este servicio y el usuario es de confianza, el propio HSS, o un dispositivo exclusivo de autenticación multimedia, puede determinar una autenticación implícita para ese usuario. A este respecto y teniendo en cuenta que a un usuario particular se le pueden dar una seriede identificadores de usuario en el dominio multimedia, la autenticación implícita a la que se hace referencia a continuación, y descrita bajo diferentes realizaciones, se puede aplicar a todos o a identificadores de usuario específicos en el dominio multimedia.

Adicionalmente, otra información relevante puede ser asimismo enviada a la S-CSCF en el mensaje respuesta de Cx-Put, tal como el tipo de autenticación, la información de acceso, como por ejemplo la dirección IP y la información de contacto, la marca de tiempo de autenticación y otros datos significativos para proporcionar un soporte de seguridad adicional.

De acuerdo con una realización de la invención comentada anteriormente, se puede notificar al usuario, una autenticación implícita propuesta por la red y prevista para que el usuario la acepte o no. Por lo tanto, la S-CSCF envía al agente de usuario de SIP un nuevo mensaje de SIP denominado "autenticación implícita SIP 4xx" en la especificación instantánea de modo que el agente de usuario de SIP, si se encuentra aceptable, inhabilita internamente el procedimiento de autenticación explícita multimedia convencionalmente llevado a cabo. Es decir, el agente de usuario de SIP no debe esperar, o espera recibir, ya sea un mensaje de pregunta de autenticación o vectores de autenticación, tal como se describe en el documento 3G TS 33.203. Además, el agente de usuario de SIP o, de manera más general, el equipo de usuario considerará que la red que soporta el dominio multimedia está implícitamente autenticada. Por otra parte, el agente de usuario de SIP podría considerar que la autenticación implícita no es aceptable, en cuyo caso se envía un acuse de recibo negativo apropiado no mostrado en ningún dibujo, a la red, con el fin de forzar un mecanismo de autenticación explícita convencional de acuerdo con el estándar aplicable anterior.

Aún haciendo referencia a la figura 3, una vez que el agente de usuario de SIP ha aceptado la autenticación implícita, responde a este mensaje con un nuevo mensaje de inicio de sesión de SIP.

En esta etapa, se puede ser consciente de que gracias a la autenticación implícita realizada de acuerdo con la invención mediante la reutilización en los datos de autenticación del dominio multimedia de una red de acceso de confianza, la presente invención proporciona asimismo una solución ventajosa para soportar autenticación única (SSO - Single Sign-On, en inglés) en el dominio multimedia para usuarios que habían sido ya autenticados por una red de acceso antes de acceder a dicho dominio multimedia.

En línea con esta ventajosa solución, la figura 3 muestra que el Inicio de sesión de SIP finalmente enviado desde el agente de usuario de SIP del equipo de usuario a la S-CSCF incluye una indicación de "SSO habilitada" destinada a indicar a la red que la autenticación implícita se ha aceptado. La red envía dicho mensaje de inicio de sesión de SIP a la CSCF que a su vez devuelve un resultado satisfactorio "SIP 200 OK" al equipo de usuario. El usuario final está ahora registrado en el dominio multimedia sin que se produzcan esos procesos de autenticación periódica adicionales en todo el inicio de sesión multimedia del usuario final.

En general, para esto y también aplicable para otras realizaciones descritas, y siempre que haya una notificación del equipo de usuario sobre una autenticación implícita, la entidad de servicio (S-CSCF) podría comprobar si otros datos relevantes, incluidos respectivamente en el inicio de sesión de SIP y en la respuesta de Cx-Put, son coincidentes con respecto a la autenticación implícita y acceso de autenticación única. Dichos datos relevantes pueden ser, por ejemplo, un tipo de autenticación, información de acceso como, por ejemplo, dirección IP e información de contacto, una marca de tiempo de autenticación o combinaciones de los mismos y otros datos significativos para proporcionar un soporte de seguridad adicional.

Aún bajo el escenario anterior en el que un usuario ha sido autenticado por una red UMTS y accede de nuevo al dominio multimedia a través de una red GPRS, y de acuerdo con una segunda realización mostrada en la figura 4, se proporciona un mecanismo aún más simplificado para autenticar a un usuario en el dominio multimedia en el que el usuario acaba de ser informado de una decisión adoptada por la red para llevar a cabo una autentificación implícita. Bajo esta segunda realización, el usuario se conecta a la red UMTS y se autentica en ella con la participación del servidor de abonados domésticos (HSS), un contexto de PDP se activa con las entidades GPRS (SGSN, GGSN) y un mensaje de inicio de sesión de SIP se envía hacia las entidades de función de control de estado de la llamada (P-CSCF, I-CSCF, S-CSCF) para registrarse en el dominio multimedia de una manera similar a la realizada en la primera realización La diferencia entre estas primera y segunda realizaciones es que el propio HSS, o un dispositivo exclusivo de autenticación multimedia, adopta la decisión final de llevar a cabo una autenticación implícita para el usuario. Con este fin, el HSS incluye una indicación "autenticación implícita por la red" en la respuesta de Cx-Put hacia la S-CSCF.

A continuación, después de haber completado un "proceso Cx-Pull" entre la S-CSCF y el HSS, y sin haber solicitado la aceptación del usuario, la S-CSCF informa al usuario de que la red ha realizado una autenticación implícita por sí misma incluyendo una indicación "autenticación implícita por la red" en una respuesta "SIP 2xx OK ", en lugar de utilizar el nuevo mensaje "SIP 4xx" anterior.

Después de recibir dicha respuesta "SIP 2xx OK" con una indicación de "autenticación implícita por la red", el agente de usuario de SIP no deberá esperar, o esperará recibir un mensaje de pregunta de autenticación o vectores de autenticación tal como se describe en el documento 3G TS 33.203. Además, el agente de usuario SIP o, de manera más general, el equipo de usuario puede considerar que la red que soporta el dominio multimedia está autenticada implícitamente, siempre que el equipo de usuario esté configurado para llevar a cabo dicha autenticación de la red.

El usuario final ha iniciado ahora sesión en el dominio multimedia sin que se produzcan estos procesos de autenticación periódica adicionales en todo el inicio de sesión multimedia del usuario final y aún con un mecanismo más sencillo que el descrito en la primera realización.

Un segundo escenario aparece cuando un usuario ha sido autenticado por una red UMTS siguiendo un procedimiento de conexión GSM y de actualización de ubicación y accede de nuevo a un dominio multimedia a través de una red GPRS. A este respecto, y en aras de la claridad, el servidor de abonados domésticos (HSS) de una red UMTS comprende toda la funcionalidad básica, y se comporta como un registro de localización de abonados domésticos (HLR – Home Location Register, en inglés) tradicional de una red GSM, más toda la funcionalidad necesaria para actuar como un servidor de abonados en un dominio multimedia. Sin embargo, siempre que la funcionalidad HLR tradicional resida en una entidad diferente que el servidor de abonado para el dominio multimedia, una interfaz adicional entre ambas entidades, a saber, el HLR de GSM y el servidor de abonado para el dominio multimedia, se utiliza para compartir datos de autenticación del usuario.

Una tercera realización en el segundo escenario anterior se muestra en la figura 5, en la que se devuelve un nuevo campo al agente de usuario de SIP del equipo de usuario durante los procedimientos de conexión y actualización de localización de GSM. Por lo tanto, el servidor de abonados (HSS) del dominio multimedia incluye una indicación de "autenticación implícita" en la operación de GSM "insertar datos de abonado" hacia el nodo de soporte de GPRS de servicio (SGSN) en la red de acceso. A continuación, el SGSN también incluye esta indicación de "autenticación implícita" en la operación de GSM "actualizar respuesta de localización" hacia el agente de usuario de SIP.

Esta indicación puede ser aplicada a todos los identificadores de usuario específicos en el dominio multimedia, y se comprende por el equipo de usuario (UE) como una invitación implícita para habilitar un acceso de autenticación única (SSO) al dominio multimedia que el equipo de usuario puede o no puede aceptar. Siempre que la autenticación implícita sea aceptable para el usuario final (UE) ya que no se requiere seguridad adicional, se envía un mensaje de inicio de sesión de SIP al dominio multimedia (P-CSCF, I-CSCF), incluyendo el mensaje de inicio de sesión de SIP una indicación de "SSO habilitada" destinada a indicar a la red que la autenticación implícita se ha aceptado.

Tras la recepción de dicho mensaje de inicio de sesión de SIP en una entidad de función de control del estado de la llamada de interrogación (I-CSCF), se incorpora la indicación de "SSO habilitada" en un nuevo campo de un mensaje "Cx-Pregunta" incluido en un procedimiento denominado "Cx-Selección-Info" mantenido con el servidor de abonados del dominio multimedia (HSS). En esta etapa, la característica "autenticación implícita para el dominio multimedia" en el propio HSS o en un dispositivo de autenticación multimedia exclusivo, procesa la indicación de "SSO habilitada" para proporcionar más datos de autenticación para el usuario tras una solicitud.

La indicación de "SSO habilitada" se incorpora asimismo en el inicio de sesión de SIP enviado desde la I-CSCF hacia la entidad de función de control del estado de la llamada de servicio (S-CSCF) actualmente seleccionada para atender al usuario. Como en realizaciones anteriores, la presente realización mostrada en la figura 5 muestra asimismo una operación "Cx-Put" llevada a cabo desde la S-CSCF al HSS. Por lo tanto, el HSS da instrucciones a la S-CSCF con una operación "Cx-Put-respuesta" que incluye una indicación de ”autenticación implícita confirmada por el usuario" con el fin de impedir una autenticación adicional del usuario final y evitar el envío de vectores de autenticación para dicho usuario final. A su vez, la S-CSCF podría comprobar asimismo si otros datos relevantes incluidos respectivamente en el inicio de sesión de SIP y en la respuesta Cx-Put son coincidentes con respecto a los datos relevantes de acceso de autenticación implícita y de inicio de sesión único, tales como tipo de autenticación, información de acceso, como por ejemplo dirección IP e información de contacto, marca de tiempo de autenticación o combinaciones de los mismos y otros datos significativos para proporcionar un soporte adicional de seguridad.

Finalmente, después de haber concluido un “Cx-Pull proceso" entre la S-CSCF y el servidor de abonado (HSS), la S-CSCF devuelve al usuario un resultado satisfactorio convencional "SIP 200 OK" hacia el agente de usuario de SIP en el equipo de usuario.

Una cuarta realización adicional en el segundo escenario anterior se muestra en la figura 6, en la que la única diferencia con la tercera realización anterior mostrada en la figura 5 es que la indicación de "autenticación implícita" se devuelve al agente de usuario de SIP del equipo de usuario en un mensaje corto enviado desde un centro de servicio de mensajes cortos (SMSC – Short Message Service Centre, en inglés) según instrucciones previas del

propio servidor de abonados (HSS), o de un dispositivo exclusivo de autenticación multimedia y, una vez que los procedimientos de conexión y autenticación GSM han terminado, en lugar de realizarse durante el procedimiento de actualización de la ubicación. Por razones de claridad en los dibujos, el par de entidades de GPRS SGSN y GGSN de la figura 5 se reemplazan por una entidad llamada "GSN" en la figura 6. Esta indicación de "autenticación implícita", como para una realización anterior, se puede aplicar asimismo a todos o a identificadores de usuario específicos en el dominio multimedia Una vez que el equipo de usuario es consciente de haber recibido esta indicación de "autenticación implícita", y siempre que dicha autenticación implícita se encuentre aceptable, el equipo de usuario procesa el mensaje e incluye una indicación de "SSO habilitada" en un mensaje de inicio de sesión de SIP que se envía para acceder al dominio multimedia (P-CSCF, I-CSCF), la indicación de "SSO habilitada" destinada a indicar a la red que la autenticación implícita ha sido aceptada por el equipo de usuario. A partir de este momento, el flujo de señalización puede ser el mismo que en la tercera realización anterior.

También en las realizaciones bajo este segundo escenario el usuario final está registrado en el dominio multimedia sin que esos procesos de autenticación periódica adicionales ocurran convencionalmente a través del inicio de sesión multimedia del usuario final y con un mecanismo más sencillo que el convencionalmente llevado a cabo.

Un tercer escenario aparece cuando un usuario que accede a través de una red de área local inalámbrica ha sido autenticado por una red UMTS y accede además al dominio multimedia a través de esta red inalámbrica de área local (WLAN).

De acuerdo con una quinta realización mostrada en la figura 7, en este tercer escenario, un usuario final está conectado y autenticado en WLAN por la red UMTS, el usuario final, o más bien el equipo de usuario (UE), ha obtenido una sesión de IP abierta preferiblemente utilizando una llamada convencionalmente denominada túnel seguro a la red doméstica. Este túnel seguro se establece preferiblemente entre el equipo de usuario y una puerta de enlace de datos en paquetes (PD-GW – Packet Data GateWay, en inglés) encapsulando datos de la sesión IP anterior, generalmente una dirección IP, dentro de la carga útil del mensaje cifrado, mientras que una dirección IP externa no relacionada con la sesión IP se utiliza entre el equipo de usuario (UE) y la puerta de enlace de datos en paquetes (PD-GW).

En esta etapa y de manera similar a la primera realización mostrada en la figura 3, el flujo de señalización en la figura 7 muestra cómo el usuario final y el agente de usuario de SIP, es decir, el equipo de usuario (UE), obtienen acceso al dominio multimedia enviando un mensaje de inicio de sesión de SIP desde el lado del usuario (UE) hacia el dominio multimedia (P-CSCF, I-CSCF).

Una entidad de función de control del estado de la llamada de interrogación (I-CSCF) inicia un procedimiento denominado convencionalmente "Cx-Selección-Info" hacia el servidor de abonados domésticos (HSS), es decir, el servidor de abonados en el dominio multimedia, para identificar una función de control del estado de la llamada de servicio (S-CSCF) actualmente a cargo del usuario. Una vez que dicha S-CSCF ha sido identificada, la I-CSCF envía un mensaje de inicio de sesión de SIP correspondiente a la S-CSCF. La S-CSCF que recibe dicho mensaje de inicio de sesión inicia un procedimiento denominado convencionalmente Cx-Put hacia el servidor de abonados domésticos (HSS).

Dado que el HSS había participado previamente en la autenticación del usuario para el acceso WLAN intercambiando un perfil de usuario y vectores de autenticación de usuario con un servidor denominado “autenticación, autorización y contabilidad” (denominado de aquí en adelante AAA-3GPP (Authentication, Authorisation and Accounting – 3GPP)), tal como se muestra en la figura 2, el HSS puede utilizar su información sobre el túnel seguro además de otra información de topología de la red para determinar la seguridad potencial de la ruta de señalización para acceder al dominio multimedia a través de dicha red de acceso. De este modo, de acuerdo con la invención, el propio HSS, o un dispositivo de autenticación multimedia exclusivo, puede decidir una autenticación implícita para dicho usuario. Esta decisión se realiza ventajosamente cuando la puerta de enlace de datos en paquetes (PD-GW) pertenece al mismo dominio doméstico que el HSS, o en otras situaciones en las que se considera que la PD-GW es segura y de confianza. Además, la característica "autenticación implícita para el dominio multimedia" puede incluir, como en realizaciones anteriores, el aprovisionamiento de datos y la configuración de datos por abonado, de tal manera que cuando un usuario tiene este servicio contratado y el usuario es de confianza, el propio HSS, o un dispositivo de autenticación multimedia exclusivo puede determinar una autenticación implícita para ese usuario.

Por lo tanto, el HSS incorpora una indicación de autenticación implícita en la “Cx-Put-respuesta” hacia la S-CSCF. Ventajosamente y en aras de la seguridad, se puede enviar asimismo otra información relevante a la S-CSCF en el mensaje "Cx-Put-respuesta", tal como tipo de autenticación, información de acceso como por ejemplo dirección IP e información de contacto, marca de tiempo de autenticación y otros datos significativos para proporcionar un soporte de seguridad adicional.

Esta quinta realización de la figura 7 está alineada con la primera realización de la figura 3 y ambas están de acuerdo con una realización de la invención comentada anteriormente, donde el usuario puede ser informado de una autenticación implícita propuesta por la red y prevista para que el usuario la acepte o no.

Por lo tanto, la S-CSCF envía al agente de usuario de SIP un nuevo mensaje de SIP denominado "autenticación implícita SIP 4xx" en la especificación instantánea, de modo que el agente de usuario de SIP, si se encuentra aceptable, deshabilita internamente el procedimiento explícito de autenticación multimedia llevado a cabo convencionalmente. Es decir, el agente de usuario de SIP no debe esperar ni esperar recibir un mensaje de pregunta de autenticación o vectores de autenticación, tal como se describe en el documento 3G TS 33.203.

Una vez que el agente de usuario de SIP ha aceptado la autenticación implícita, responde a este mensaje de "SIP 4xx autenticación implícita" con un nuevo mensaje de inicio de sesión de SIP que incluye una indicación de "SSO habilitada" prevista para indicar a la red que la autenticación implícita ha sido aceptada. La red (P-CSCF, I-CSCF) envía dicho mensaje de inicio de sesión de SIP a la S-CSCF que, a su vez, devuelve un resultado satisfactorio "SIP 200 OK" al equipo de usuario (UE). El usuario final, habiendo accedido a través de una red WLAN, está ahora registrado en el dominio multimedia sin que estos procesos de autenticación periódica adicionales ocurran típicamente durante todo el inicio de sesión multimedia del usuario final.

La descripción para la quinta realización mostrada en la figura 7 se ha hecho coincidir en lo posible con la de la primera realización mostrada en la figura 3. De manera similar, la enseñanza a partir de la segunda realización mostrada en la figura 4, en la que GPRS es la red de acceso, puede ser convenientemente aplicable a otra realización en la que WLAN es la red de acceso, no requiriendo esto último ninguna explicación adicional a la vista de las realizaciones anteriores.

Por otra parte, la tercera realización anterior, en la que el GPRS es la red de acceso, es prácticamente aplicable también a otra realización en la que WLAN es la red de acceso en la medida en que las indicaciones de autenticación relevantes enviadas al equipo de usuario se incluyen como par de valor de atributo (AVP – Attribute Value Pair, en inglés) específico en los mensajes correspondientes de un protocolo RADIUS o Diámetro utilizado por WLAN.

Finalmente, la cuarta realización anterior en la que el GPRS es la red de acceso es también aplicable a otra realización en la que WLAN es la red de acceso suponiendo un soporte para servicios de mensajes cortos (SMS) en WLAN o utilizando la tecnología de conmutación de circuitos de una infraestructura de GRPS para SMS en caso de tener terminales dobles como equipo de usuario.

Un cuarto escenario aparece cuando un usuario ha sido autenticado por una red CDMA 2000 siguiendo un procedimiento de conexión de servicio de datos en paquetes y accede a un dominio multimedia a través de una red de servicios de datos en paquetes. La figura 8 muestra una sexta realización alineada con la de la figura 4 bajo el primer escenario, en la que un servidor de autenticación, autorización y contabilidad (AAA) actúa como servidor de abonado de una red CDMA 2000. A este respecto y para mayor claridad, el servidor de autenticación, autorización y contabilidad (AAA) de la red CDMA 2000 comprende toda la funcionalidad básica requerida para permitir el acceso a los servicios de datos en paquetes en una red CDMA 2000, y toda la funcionalidad necesaria para actuar como un servidor de abonado en un dominio multimedia.

No obstante, siempre que la funcionalidad AAA tradicionalmente conocida para el acceso a servicios de datos en paquetes CDMA 2000 resida en una entidad diferente del servidor de abonado para el dominio multimedia, una interfaz adicional entre ambas entidades, a saber, entre una AAA de CDMA 2000 tradicional y el servidor de abonado para el dominio multimedia, se utiliza para compartir datos de autenticación de usuario.

Aparte de estas consideraciones, las realizaciones anteriores también son aplicables a este escenario que implica una red CDMA 2000 suponiendo que la información relevante puede ser transportada utilizando extensiones a las actuales interfaces RADIUS y Diámetro.

Una realización adicional se presenta bajo el primer escenario de ejemplo anterior y se muestra en la figura 9, en la que la propuesta para una autenticación implícita (propuesta SSO) se desencadena realmente desde el propio equipo de usuario (UE) y sin que haber recibido una invitación previa del dominio multimedia (IMS). Por lo tanto, la secuencia de flujo en la figura 9 presenta una realización alternativa a las figuras 5 y 6, en la que el equipo de usuario (UE) envía directamente al dominio multimedia (IMS) su propuesta para una autenticación implícita (Propuesta SSO), sin haber recibido la invitación anterior con un mensaje de respuesta de actualizar localización o con un servicio de mensajes cortos (SMS), y con el fin de llevar a cabo dicha autenticación implícita entre dicho equipo de usuario y el dominio multimedia.

Este nuevo enfoque se podría aplicar asimismo para modificar otras realizaciones anteriores e independientemente del escenario de aplicación.

La invención se ha descrito anteriormente con respecto a varias realizaciones de una manera ilustrativa y no restrictiva. Obviamente, modificaciones y variaciones de la presente invención son posibles a la luz de las enseñanzas anteriores, y cualquier modificación de las realizaciones que se encuentre dentro del alcance de las reivindicaciones está destinada a ser incluida en ellas.

A continuación, se describen otras realizaciones.

Realización 1: Un dispositivo para la autenticación multimedia de un usuario (UE) que accede a un dominio multimedia (IMS) a través de una red de acceso (UMTS; WLAN; GPRS; CDMA 2000), el dispositivo para su uso en, o en cooperación con un servidor de abonado (HSS; AAA) de la red de acceso que guarda los datos de autenticación para el usuario y es accesible para el dominio multimedia (IMS), comprendiendo el dispositivo: un medio para decidir que una autenticación implícita entre el usuario (UE) y el dominio multimedia (IMS) puede tener lugar, evitando de este modo las necesidades de una autenticación explícita; y medios para dar instrucciones a una entidad de servicio (S-CSCF) encargada de autenticar al usuario (UE) en el dominio multimedia (IMS) de que puede tener lugar la autentificación implícita.

Realización 2: El dispositivo de la realización 1 en el que el medio para decidir que puede tener lugar una autentificación implícita incluye medios para determinar la seguridad potencial de la ruta de señalización para acceder al dominio multimedia a través de dicha red de acceso.

Realización 3: El dispositivo de la realización. 1, en el que los medios para dar instrucciones a la entidad de servicio de que puede tener lugar una autenticación implícita incluyen medios para indicar (autenticación implícita) que la decisión final está en el lado del usuario (UE) que podría forzar una autenticación explícita.

Realización 4: El dispositivo de la realización 1, en el que los medios para dar instrucciones a la entidad de servicio de que puede tener lugar una autenticación implícita incluyen medios para indicar (autenticación implícita por la red) que esta es una decisión final adoptada por la red y no se puede llevar a cabo ninguna autenticación explícita.

Realización 5: El dispositivo de la realización 1, que incluye además un medio (autenticación implícita, autenticación implícita por la red) para notificar al equipo de usuario que una autenticación implícita del usuario para acceder al dominio multimedia puede ser realizada por la red.

Realización 6: El dispositivo de la realización 1, en el que el medio para decidir que puede tener lugar una autenticación implícita entre el usuario (UE) y el dominio multimedia (IMS) incluye medios para recibir una propuesta de autenticación implícita (propuesta de SSO) originada en el equipo de usuario (UE).

Realización 7: El dispositivo de la realización 3, que comprende además medios para recibir una indicación (SSO activada) originada en el equipo de usuario (UE) para confirmar la aceptación de la autenticación implícita propuesta por la red.

Realización 8: El dispositivo de la realización 7, que comprende además medios para indicar (autenticación implícita confirmada por el usuario) a la entidad de servicio (S-CSCF) encargada de autenticar al usuario en el dominio multimedia (IMS) que el usuario ha confirmado la autenticación.

Realización 9: El dispositivo de la realización 8, que comprende además medios para proporcionar datos de autenticación adicionales a dicha entidad de servicio (S-CSCF), incluyendo dichos datos de autenticación adicionales al menos un elemento seleccionado de un grupo de elementos que comprende: tipo de autenticación: información de acceso; y marca de tiempo de autenticación.

Realización 10: Un equipo de usuario (UE) habilitado para obtener acceso a un dominio multimedia (IMS) a través de una red de acceso (UMTS; WLAN; GPRS; CDMA 2000), y dispuesto para llevar a cabo un primer procedimiento de autenticación explícita con la red de acceso y un segundo procedimiento de autenticación explícita con el dominio multimedia (IMS), comprendiendo el equipo de usuario (UE) medios para el procesamiento de al menos una notificación seleccionada de un grupo de notificaciones que incluye: una notificación (autenticación implícita, autenticación implícita por la red) recibida desde el dominio multimedia (IMS) indicando que la red puede llevar a cabo una autenticación implícita para el usuario; y una notificación (propuesta de SSO) propuesta desde el equipo de usuario (UE) hacia el dominio multimedia (IMS) para llevar a cabo una autenticación implícita entre dicho equipo de usuario y el dominio multimedia.

Realización 11: El equipo de usuario (UE) de la realización 10, en el que los elementos para procesar una notificación recibida desde el dominio multimedia (IMS) incluyen medios para recibir y procesar una indicación (autenticación implícita) de que la decisión final está en el equipo de usuario (UE), que podría forzar una autenticación explícita.

Realización 12: El equipo de usuario (UE) de la realización 11, que comprende además medios para enviar hacia el dominio de multimedia (IMS) una indicación (SSO habilitada) para confirmar la aceptación de la autenticación implícita propuesta por la red.

Realización 13: El equipo de usuario (UE) de la realización 12, que comprende además medios para proporcionar datos de autenticación adicionales al dominio multimedia (IMS), comprendiendo dichos datos de autenticación adicionales al menos un elemento seleccionado de un grupo de elementos que comprende: tipo de autenticación; información de acceso; y marca de tiempo de autenticación.

Realización 14: Equipo de usuario (UE) de la realización 10, en el que el medio para procesar una notificación recibida del dominio multimedia (IMS) incluye medios para recibir y procesar una indicación (autenticación implícita

por la red) de que la autenticación implícita es una decisión final adoptada por la red y no se puede realizar ninguna autenticación explícita.

Realización 15: Método para autenticar a un usuario (UE) que accede a un dominio multimedia (IMS) a través de una red de acceso (UMTS; WLAN; GPRS; CDMA 2000), comprendiendo el método las etapas de: autenticar al usuario en la red de acceso (UMTS; WLAN; GPRS; CDMA 2000) a través de la que el usuario accede, teniendo la red de acceso un servidor de abonado (HSS; AAA) con datos de autenticación para el usuario y accesible al dominio multimedia (IMS); registrar el usuario (UE) en el dominio multimedia (IMS); decidir que puede tener lugar una autenticación implícita entre el usuario (UE) y el dominio multimedia (IMS), evitando así las necesidades de una autenticación explícita; y dar instrucciones a una entidad de servicio (S-CSCF) encargada de autenticar al usuario (UE) en el dominio multimedia (IMS) de que puede tener lugar la autentificación implícita.

Realización 16: El método de la realización 15, que comprende además una etapa de notificar desde el dominio multimedia (IMS) (autenticación implícita; autenticación implícita por la red) al equipo de usuario (UE) que se puede realizar una autenticación implícita del usuario para acceder al dominio multimedia.

Realización 17: El método de la realización 15, en el que la etapa de decidir que puede tener lugar una autenticación implícita incluye una etapa de determinar la seguridad potencial de la ruta de señalización para acceder al dominio multimedia a través de dicha red de acceso.

Realización 18: El método de la realización 15, en el que la etapa de decidir que puede tener lugar una autenticación implícita incluye una etapa de proponer desde el equipo de usuario (UE) al dominio multimedia (IMS) una autenticación implícita que se llevará a cabo entre dicho equipo de usuario y el dominio multimedia.

Realización 19: El método de la realización 15, en el que la etapa de dar instrucciones a la entidad de servicio de que puede tener lugar una autentificación implícita incluye una etapa de indicar (autenticación implícita por la red) que esta es una decisión final adoptada por la red y no se puede llevar a cabo una autenticación explícita.

Realización 20: El método de la realización 15, en el que la etapa de indicar a la entidad de servicio que puede tener lugar una autenticación implícita incluye una etapa de indicar (autenticación implícita) que la decisión final está en el equipo de usuario, que podría forzar una autenticación explícita.

Realización 21: El método de la realización 20, que comprende además una etapa de confirmar (SSO activada) desde el equipo de usuario (UE) la aceptación de una autenticación implícita propuesta por la red.

Realización 22: El método de la realización 21, que comprende además una etapa de indicar (autenticación implícita confirmada por el usuario) a la entidad de servicio (S-CSCF) encargada de autenticar al usuario (UE) en el dominio multimedia (IMS) que el usuario ha confirmado la autenticación implícita.

Realización 23: Una entidad de servicio (S-CSCF) encargada de autenticar a un usuario (UE) en el dominio multimedia (IMS) cuando el usuario accede al mismo a través de una red de acceso (UMTS; WLAN; GPRS; CDMA 2000) en la que dicho usuario ha sido autenticado previamente, comprendiendo la entidad de servicio (S-CSCF): medios para recibir y procesar instrucciones (autenticación implícita, autenticación implícita por la red) originados en el dispositivo de la realización 1 que indican que puede tener lugar una autentificación implícita; y un medio para notificar (autenticación implícita, autenticación implícita por la red) a un equipo de usuario (UE) que una autenticación implícita del usuario para acceder al dominio multimedia (IMS) puede ser llevada a cabo por la red.

Realización 24: La entidad de servicio (S-CSCF) de la realización 23, que comprende también medios para recibir una indicación (SSO habilitada) originada en el equipo de usuario (UE) de la realización 12 para confirmar la aceptación de una autenticación implícita propuesta por la red.

Realización 25: La entidad de servicio (S-CSCF) de la realización 23, que comprende además medios para recibir una indicación (autenticación implícita confirmada por el usuario) originada en el dispositivo de la realización 8 que indica que el usuario ha confirmado la autenticación implícita.

Realización 26: La entidad de servicio (S-CSCF) de la realización 25, que comprende además medios para comprobar la coincidencia de datos de autenticación adicionales recibidos respectivamente desde el dispositivo de la realización 9 y desde el equipo de usuario de la realización 13 con el fin de proporcionar un soporte de seguridad adicional.

Realización 27: La entidad de servicio (S-CSCF) de la realización 26, en la que dichos datos de autenticación adicionales incluyen al menos un elemento seleccionado de un grupo de elementos que comprende: tipo de autenticación; información de acceso; y marca de tiempo de autenticación.

Realización 28: La entidad de servicio (S-CSCF) de la realización 23, en la que el medio para notificar al usuario (UE) que una autenticación implícita puede ser llevada a cabo por la red incluye medios para indicar (autenticación implícita por la red) al usuario (UE) que la autenticación implícita es una decisión final adoptada por la red y no se puede realizar una autenticación explícita.

Realización 29: Una entidad de servidor de proximidad (P-CSCF) prevista para actuar como punto de entrada en el dominio multimedia (IMS) para usuarios (UE) que acceden a él a través de una red de acceso (UMTS; WLAN; GPRS; CDMA 2000) en la que el usuario había sido autenticado previamente, y que comprende medios para procesar al menos una notificación seleccionada de un grupo de notificaciones que incluyen: una notificación (autenticación implícita, autenticación implícita por la red) enviada al equipo de usuario (UE) para indicar que una autenticación implícita del usuario para acceder al dominio multimedia (IMS) puede ser llevada a cabo por la red; y una notificación (propuesta de SSO) recibida del equipo de usuario (UE) para proponer una autenticación implícita al dominio multimedia (IMS) entre dicho equipo de usuario y el dominio multimedia.

Realización 30: La entidad de servidor de proximidad (P-CSCF) de la realización 29, que comprende además medios para recibir una indicación (SSO habilitada) desde el equipo de usuario (UE) de que acepta la autenticación implícita propuesta por la red.

Realización 31: La entidad de servidor de proximidad (P-CSCF) de la realización 29, que comprende además medios para indicar (autenticación implícita por la red) al usuario (UE) que la autenticación implícita es una decisión final adoptada por la red y no se puede llevar a cabo ninguna autenticación explícita.

Realización 32: Una entidad de interrogación (I-CSCF) que consulta a un servidor de abonado (HSS; AAA-3GPP) en el dominio multimedia (IMS) sobre un usuario (UE) que ha accedido a dicho dominio multimedia a través de una red de acceso (WLAN, GPRS), teniendo la entidad de interrogación medios para recibir una solicitud de inicio de sesión del usuario, y medios para acusar el recibo de dicho inicio de sesión hacia el usuario, y que comprende medios para transmitir una indicación (autenticación implícita, autenticación implícita por la red) hacia el usuario (UE) de que se puede llevar a cabo una autenticación implícita del usuario para acceder al dominio multimedia (IMS).

Realización 33: La entidad de interrogación (I-CSCF) de la realización 32, que comprende, además: medios para recibir una indicación (SSO habilitada; SSO propuesta) originada en el equipo de usuario (UE) para permitir una autenticación implícita; y medios para transmitir dicha indicación desde el equipo de usuario hacia al menos una entidad seleccionada de un grupo de entidades que comprende el dispositivo de la realización 1 y la entidad de servicio (S-CSCF) de la realización 23.

Realización 34: La entidad de interrogación (I-CSCF) de la realización 32, que comprende además medios para transmitir al usuario (UE) una indicación (autenticación implícita por la red) de que la autenticación implícita es una decisión final adoptada por la red y no se puede llevar a cabo ninguna autenticación explícita.

REIVINDICACIONES

1. Equipo de usuario, UE, habilitado para acceder a un dominio multimedia (IMS) a través de una red de acceso (GSM/UMTS; WLAN;), dispuesto para llevar a cabo un procedimiento de autenticación explícito con la red de acceso, y **caracterizado por** estar dispuesto además para enviar un mensaje de inicio de sesión indicando que se propone un procedimiento de autenticación implícita con el dominio multimedia (IMS) desde el UE.

2. Equipo de usuario según la reivindicación 1, en el que el procedimiento de autenticación implícita con el dominio multimedia (IMS) se basa en el procedimiento de autenticación explícita anterior llevado a cabo con la red de acceso.

3. Equipo de usuario según la reivindicación 2, en el que el procedimiento de autenticación explícita con la red de acceso es un mecanismo de autentificación AKA.

4. Equipo de usuario según la reivindicación la reivindicación 3, en el que el mecanismo de autenticación AKA llevado a cabo con la red de acceso es uno de: SIM AKA, USIM AKA y EAP AKA.

5. Equipo de usuario según cualquiera de las reivindicaciones 1 a 4, en el que el mensaje de inicio de sesión es un mensaje de inicio de sesión de protocolo de inicio de sesión, en lo sucesivo en esta memoria, SIP.

6. Equipo de usuario según la reivindicación la reivindicación 5, que comprende además medios para recibir desde el dominio multimedia (IMS), en respuesta al mensaje de inicio de sesión de SIP, un mensaje de SIP 200 OK.

7. Equipo de usuario según la reivindicación 6, en el que el mensaje SIP 200 OK indica un resultado de autentificación implícita satisfactoria.

8. Equipo de usuario según cualquiera de las reivindicaciones 1 a 8, en el que el equipo de usuario está dispuesto para llevar a cabo un procedimiento de autenticación explícita con el dominio multimedia (IMS) mediante la emisión de un mensaje de inicio de sesión adicional para una identidad privada dada.

9. Equipo de usuario según la reivindicación 8, en el que el procedimiento de autenticación explícita con el dominio multimedia (IMS) es un mecanismo de autenticación AKA.

10. Método para un equipo de usuario, UE, que obtiene acceso a un dominio multimedia (IMS) a través de una red de acceso (GSM/UMTS; WLAN;), comprendiendo el método que:

- el equipo de usuario lleva a cabo un procedimiento de autenticación explícita con la red de acceso; y

caracterizado por que:

el equipo de usuario emite un mensaje de inicio de sesión que indica que desde el UE se propone un procedimiento de autenticación implícita con el dominio multimedia (IMS).

11. Método según la reivindicación 10, en el que el procedimiento de autenticación implícita con el dominio multimedia (IMS) se basa en el procedimiento de autenticación explícita anterior llevado a cabo con la red de acceso.

12. Método según la reivindicación 11, en el que el procedimiento de autenticación explícita con la red de acceso es un mecanismo de autenticación AKA.

13. Método según la reivindicación 12, en el que el mecanismo de autenticación AKA llevado a cabo con la red de acceso es uno de: SIM AKA, USIM AKA y EAP AKA.

14. Método según cualquiera de las reivindicaciones 10 a 13, en el que los mensajes de inicio de sesión son mensajes de inicio de sesión de protocolo de inicio de sesión, en lo sucesivo en esta memoria, SIP.

15. Método según la reivindicación 14, que comprende además que el equipo de usuario recibe desde el dominio multimedia (IMS), en respuesta al mensaje de inicio de sesión de SIP, un mensaje de SIP 200 OK.

16. Método según la reivindicación 15, en el que el mensaje SIP 200 OK indica un resultado de autenticación implícita satisfactoria.

17. Método según cualquiera de las reivindicaciones 11 a 16, que comprende además que el equipo de usuario realiza un procedimiento de autenticación explícito con el dominio multimedia (IMS) emitiendo un mensaje de inicio de sesión adicional para una identidad privada dada.

18. Método según la reivindicación 17, en el que el procedimiento de autenticación explícita con el dominio multimedia (IMS) es un mecanismo de autenticación AKA.

19. Sistema para proporcionar a un equipo de usuario, UE, acceso a un dominio multimedia (IMS) a través de una red de acceso, comprendiendo el sistema el dominio multimedia (IMS), la red de acceso y el equipo de usuario (UE) de cualquiera de las reivindicaciones 1 a 9.

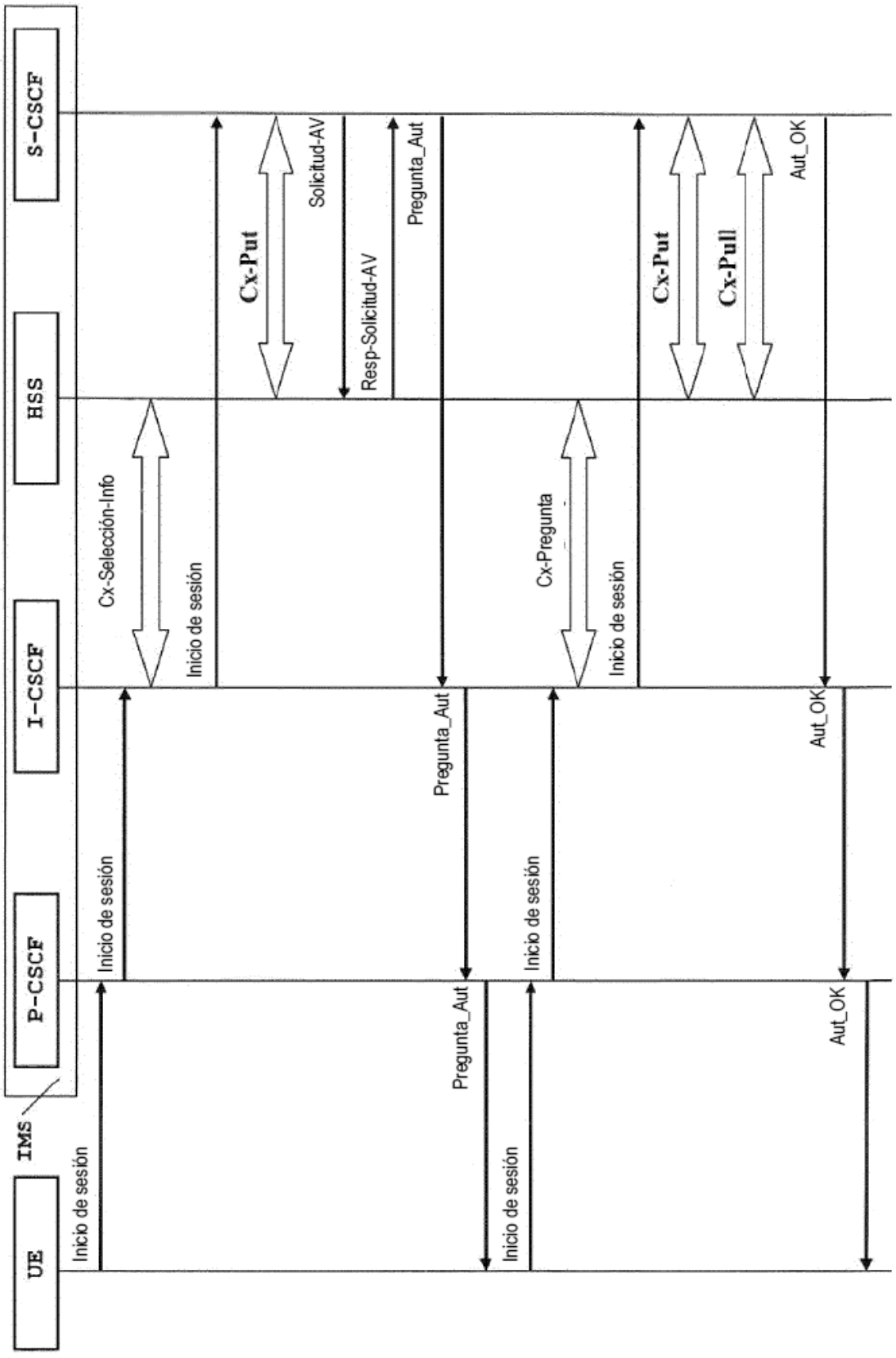

Figura -1- Estado de la técnica

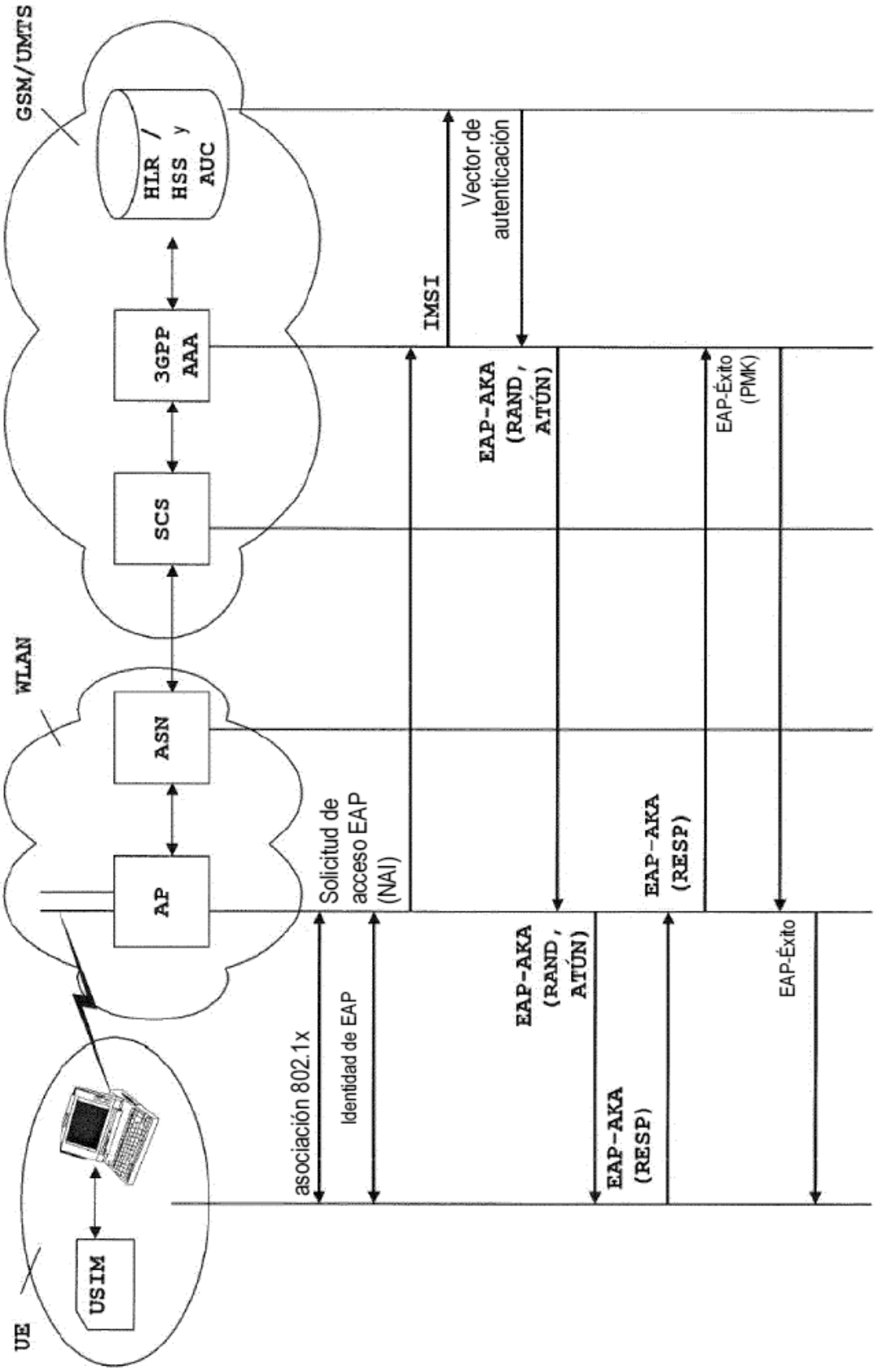

Figura –2- Estado de la técnica

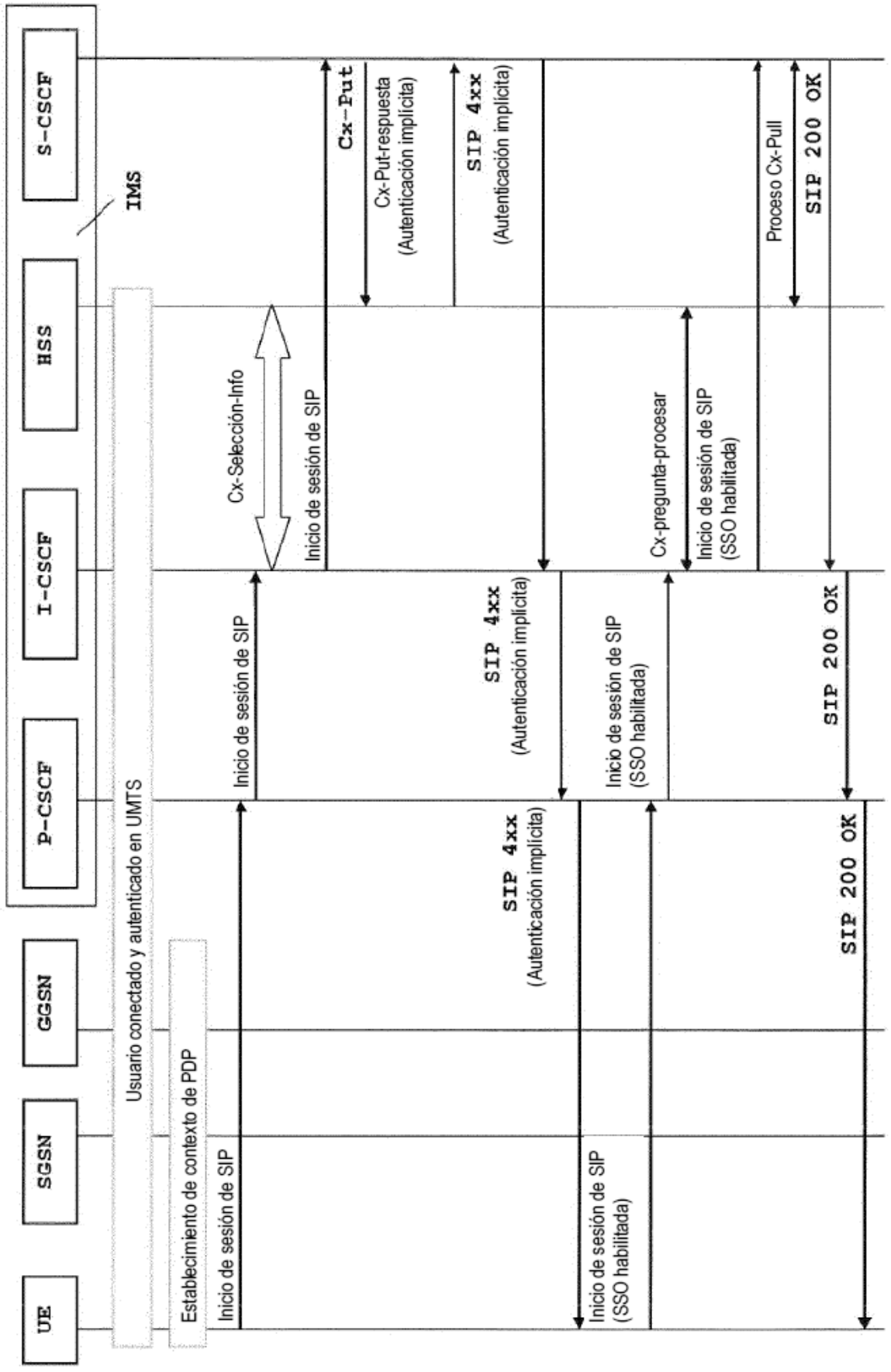
UE
SGSN
GGSN
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuario conectado y autenticado en UMTS
Establecimiento de contexto de PDP
Inicio de sesión de SIP
Inicio de sesión de SIP
Cx-Selección-Info
Inicio de sesión de SIP
Cx-Put
Cx-Put-respuesta (Autenticación implícita)
SIP 4xx (Autenticación implícita)
SIP 4xx (Autenticación implícita)
Inicio de sesión de SIP (SSO habilitada)
Cx-pregunta-procesar
Inicio de sesión de SIP (SSO habilitada)
Proceso Cx-Pull
SIP 200 OK
SIP 200 OK
SIP 200 OK

Figura -3-

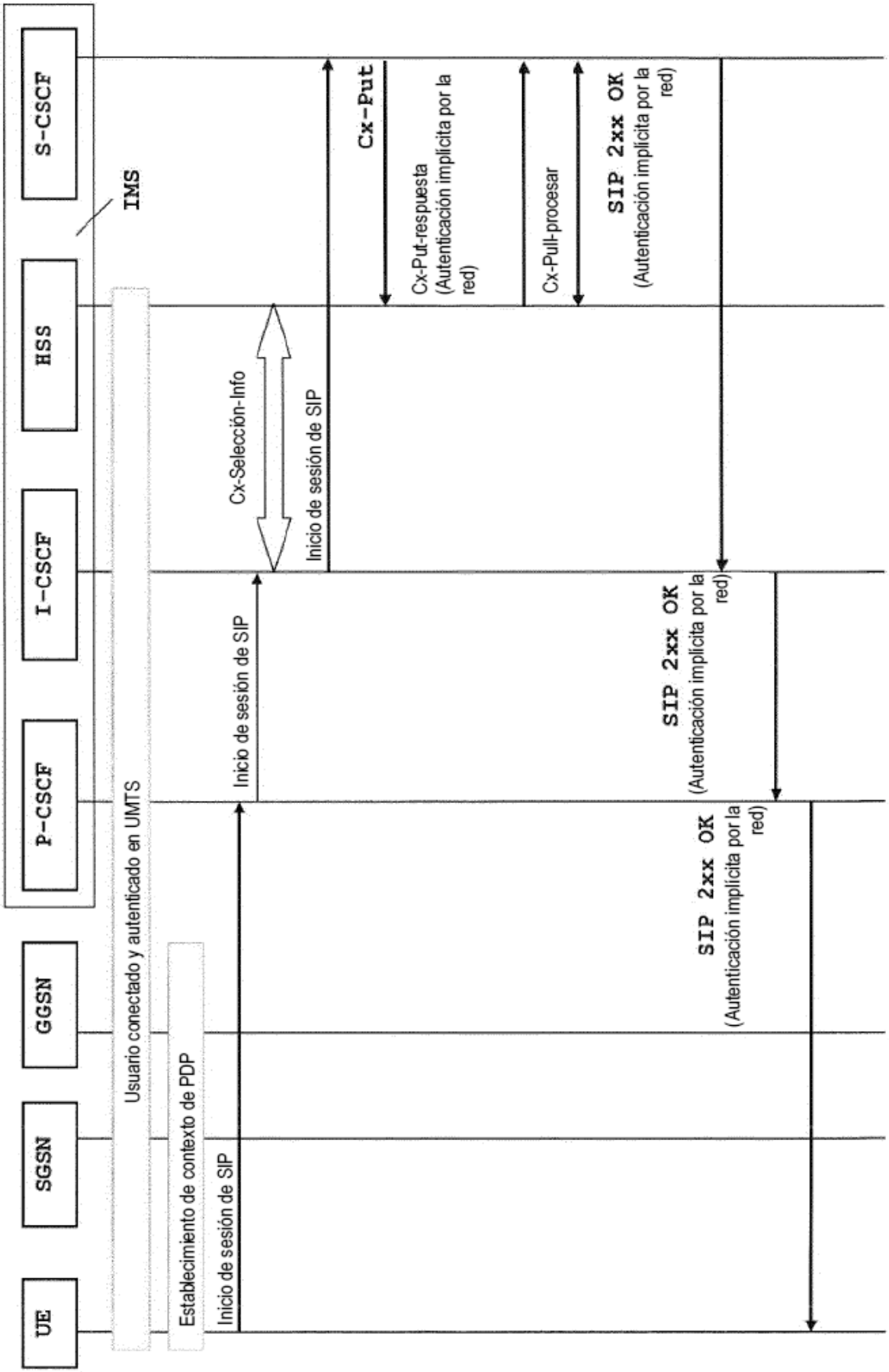
UE
SGSN
GGSN
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuario conectado y autenticado en UMTS
Establecimiento de contexto de PDP
Inicio de sesión de SIP
Inicio de sesión de SIP
Cx-Selección-Info
Inicio de sesión de SIP
Cx-Put
Cx-Put-respuesta (Autenticación implícita por la red)
Cx-Pull-procesar
SIP 2xx OK (Autenticación implícita por la red)
SIP 2xx OK (Autenticación implícita por la red)
SIP 2xx OK (Autenticación implícita por la red)

Figura -4-

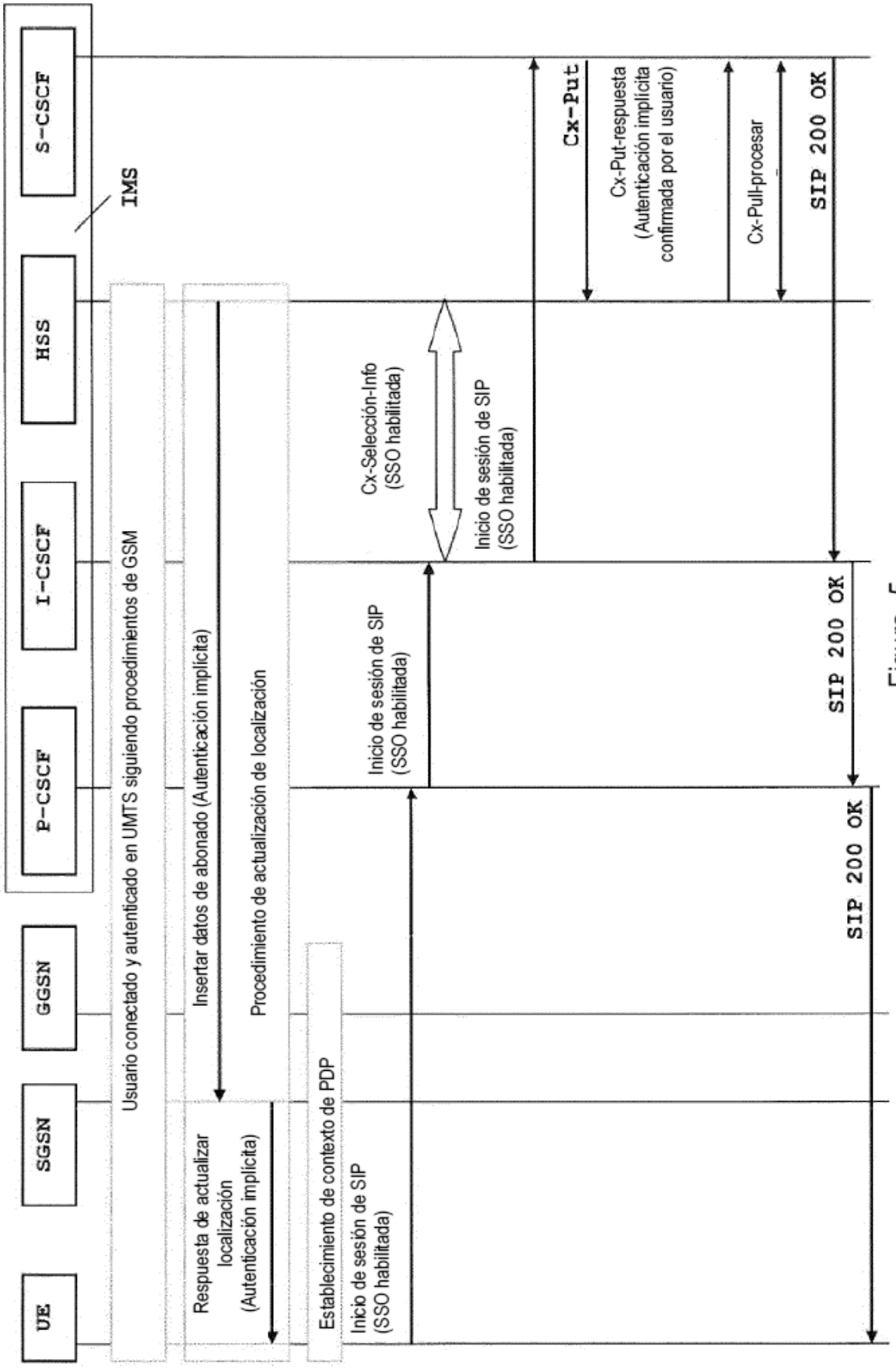
UE
SGSN
GGSN
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuario conectado y autenticado en UMTS siguiendo procedimientos de GSM
Insertar datos de abonado (Autenticación implícita)
Respuesta de actualizar localización (Autenticación implícita)
Procedimiento de actualización de localización
Establecimiento de contexto de PDP
Inicio de sesión de SIP (SSO habilitada)
Inicio de sesión de SIP (SSO habilitada)
Cx-Selección-Info (SSO habilitada)
Inicio de sesión de SIP (SSO habilitada)
Cx-Put
Cx-Put-respuesta (Autenticación implícita confirmada por el usuario)
Cx-Pull-procesar
SIP 200 OK
SIP 200 OK
SIP 200 OK

Figura -5-

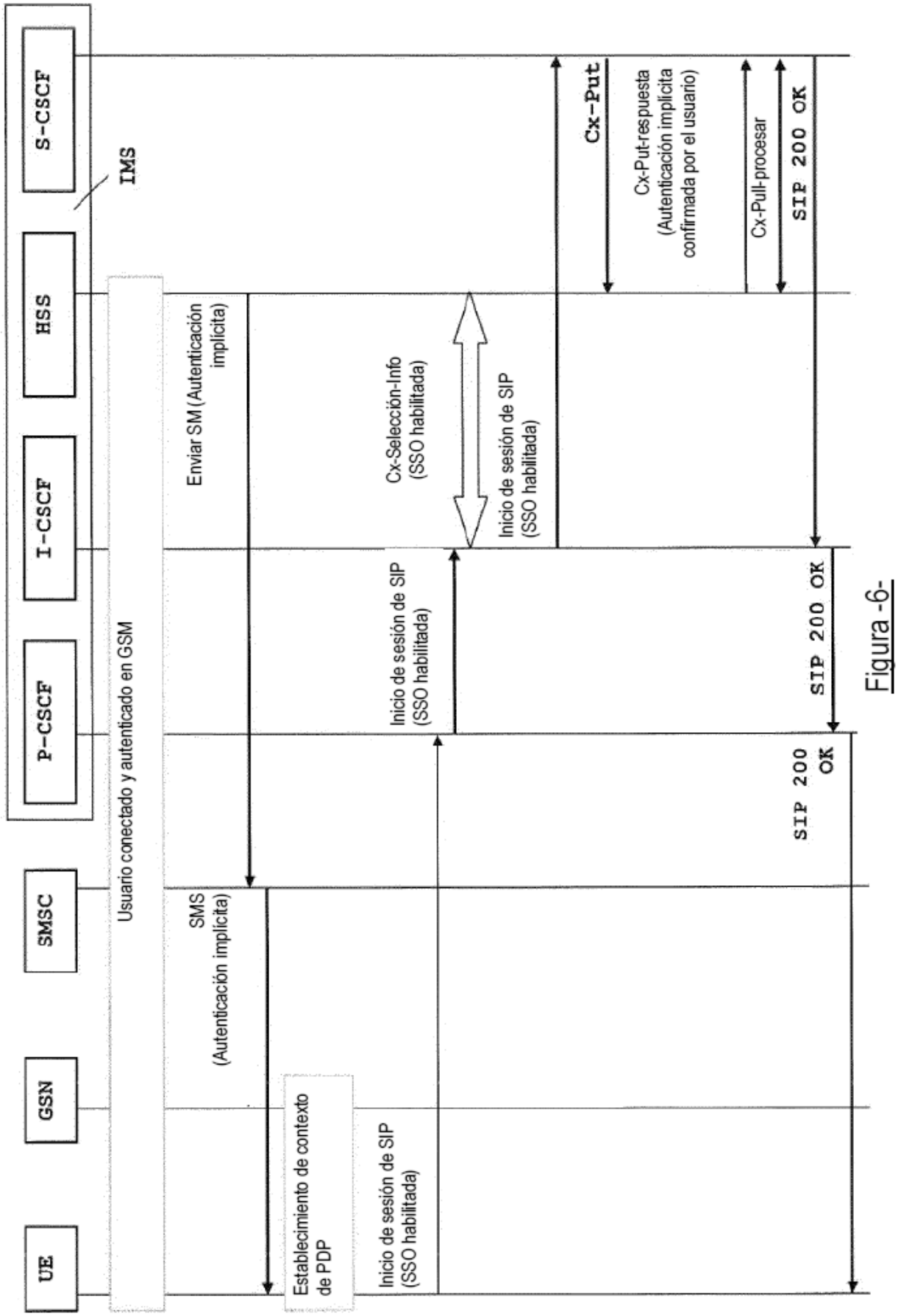
UE
GSN
SMSC
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuario conectado y autenticado en GSM
SMS (Autenticación implícita)
Establecimiento de contexto de PDP
Inicio de sesión de SIP (SSO habilitada)
Enviar SM (Autenticación implícita)
Inicio de sesión de SIP (SSO habilitada)
Cx-Selección-Info (SSO habilitada)
Inicio de sesión de SIP (SSO habilitada)
SIP 200 OK
SIP 200 OK
Cx-Put
Cx-Put-respuesta (Autenticación implícita confirmada por el usuario)
Cx-Pull-procesar
SIP 200 OK

Figura -6-

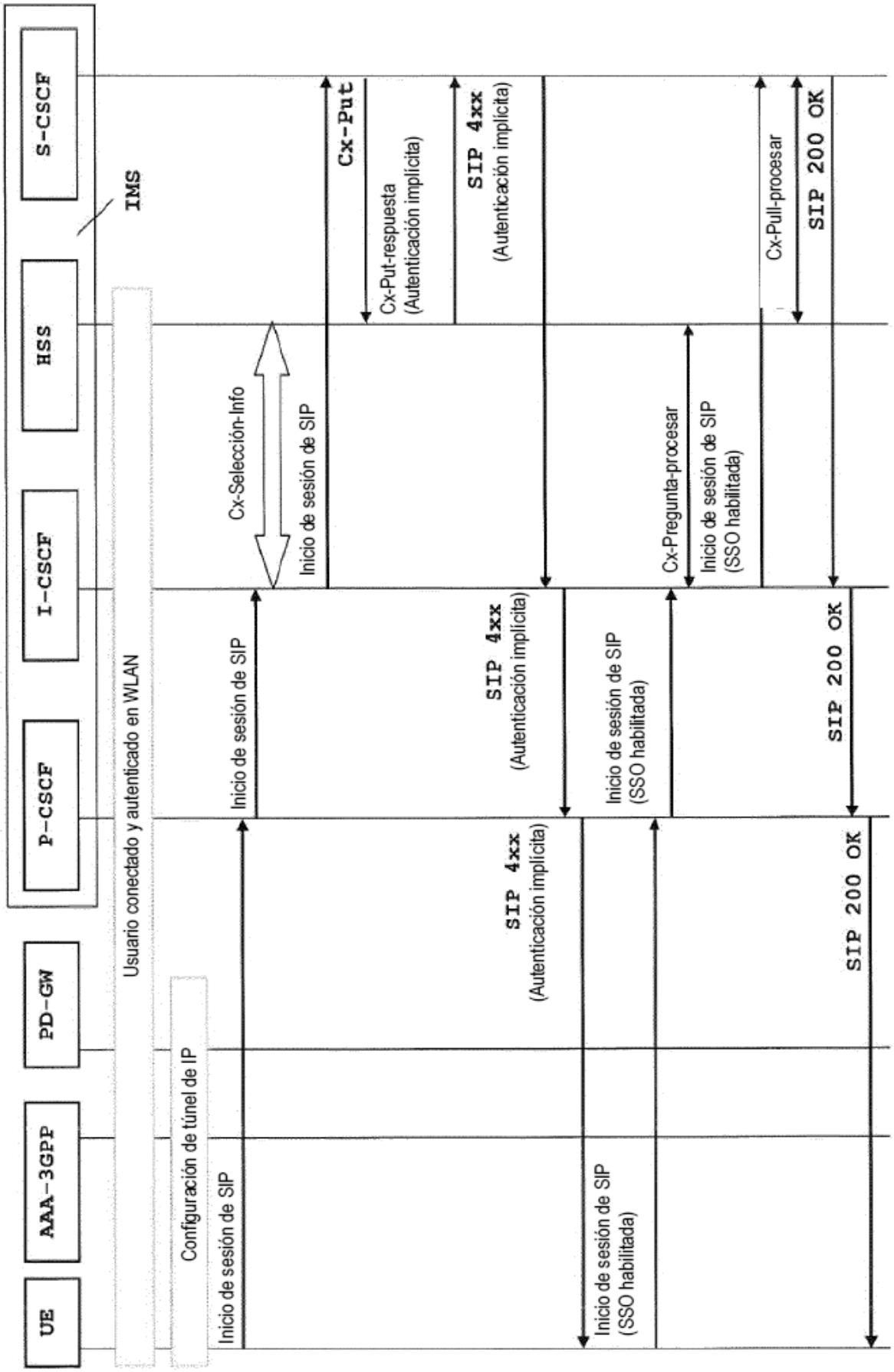
UE
AAA-3GPP
PD-GW
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuario conectado y autenticado en WLAN
Configuración de túnel de IP
Inicio de sesión de SIP
Inicio de sesión de SIP
SIP 4xx
(Autenticación implícita)
Inicio de sesión de SIP
(SSO habilitada)
SIP 200 OK
Cx-Selección-Info
Inicio de sesión de SIP
Cx-Put
Cx-Put-respuesta
(Autenticación implícita)
SIP 4xx
(Autenticación implícita)
Cx-Pregunta-procesar
Inicio de sesión de SIP
(SSO habilitada)
Cx-Pull-procesar
SIP 200 OK

Figura -7-

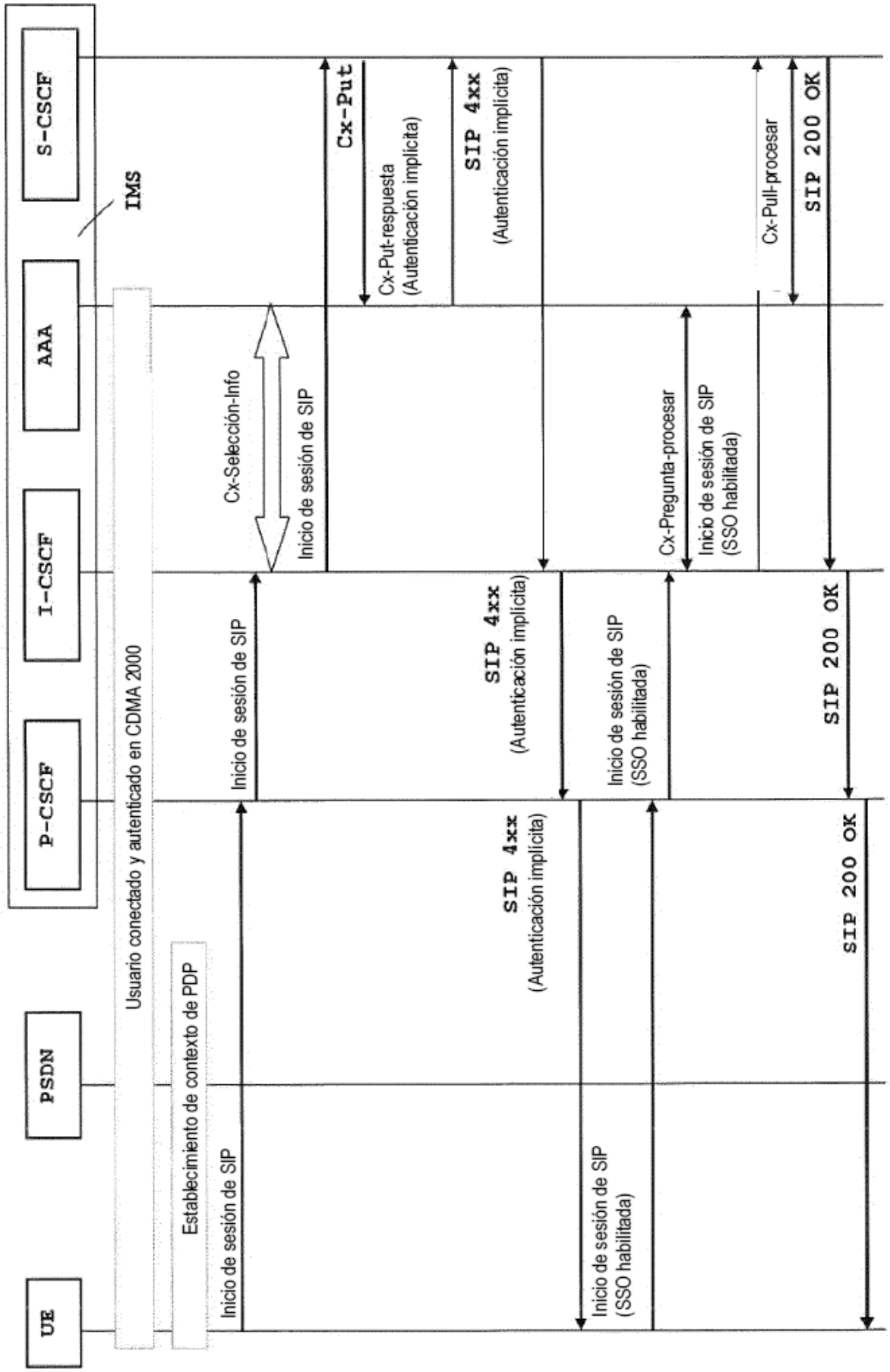
UE
PSDN
P-CSCF
I-CSCF
AAA
S-CSCF
IMS
Usuario conectado y autenticado en CDMA 2000
Establecimiento de contexto de PDP
Inicio de sesión de SIP
Inicio de sesión de SIP
SIP 4xx
(Autenticación implícita)
Inicio de sesión de SIP
(SSO habilitada)
SIP 200 OK
Cx-Selección-Info
Inicio de sesión de SIP
Cx-Put
Cx-Put-respuesta
(Autenticación implícita)
SIP 4xx
(Autenticación implícita)
Cx-Pregunta-procesar
Inicio de sesión de SIP
(SSO habilitada)
Cx-Pull-procesar
SIP 200 OK

Figura -8-

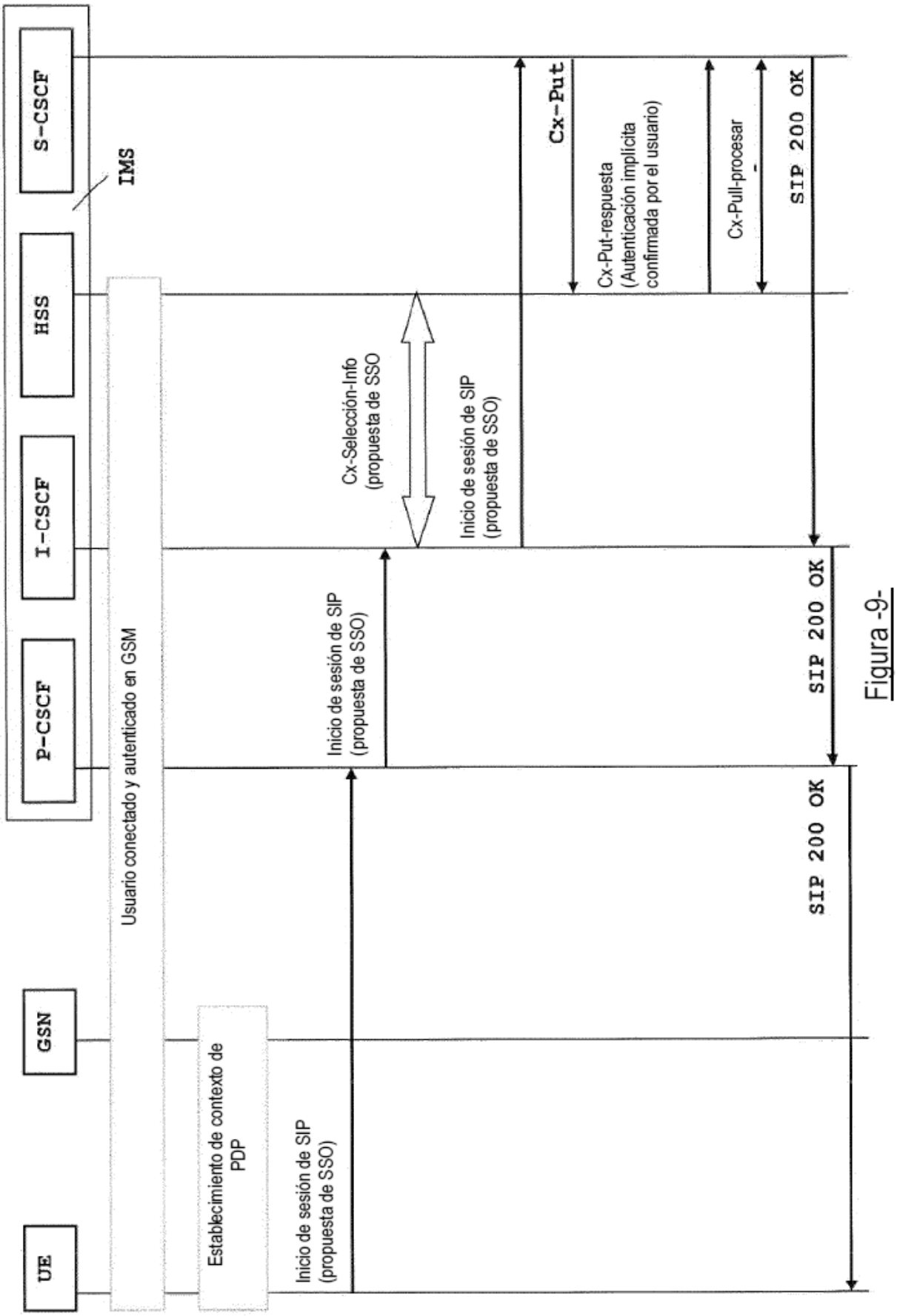
UE
GSN
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuario conectado y autenticado en GSM
Establecimiento de contexto de PDP
Inicio de sesión de SIP (propuesta de SSO)
Inicio de sesión de SIP (propuesta de SSO)
Cx-Selección-Info (propuesta de SSO
Inicio de sesión de SIP (propuesta de SSO)
Cx-Put
Cx-Put-respuesta (Autenticación implícita confirmada por el usuario)
Cx-Pull-procesar
SIP 200 OK
SIP 200 OK
SIP 200 OK

Figura -9-