(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 472 425**

(51) Int. CI.:

H04W 48/14 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.01.2010 E 10731045 (0)**

(97) Fecha y número de publicación de la concesión europea: **02.04.2014 EP 2389024**

(54) Título: **Sistema de comunicación, entidad de control del acceso y método para controlar el acceso de un equipo de usuario**

(30) Prioridad:

13.01.2009 CN 200910003638

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.07.2014

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
B1-3A Intellectual Property Dept. Huawei Administration Building Bantian Longgang Shenzhen
Guangdong 518129 , CN

(72) Inventor/es:

HAN, GUANGLIN;
ZHANG, PENG y
ZHOU, ZHENG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema de comunicación, entidad de control del acceso y método para controlar el acceso de un equipo de usuario

CAMPO DE LA INVENCIÓN

La presente invención se refiere a tecnologías de comunicaciones y en particular, a un sistema de comunicación, una entidad de control del acceso y un método para controlar el acceso de equipo de usuario.

ANTECEDENTES DE LA INVENCIÓN

En un UMTS (Universal Mobile Telecommunications System, Sistema de Comunicación Móvil Universal) y una red LTE (Long Term Evolution, Evolución a Largo Plazo) antes de que el equipo UE (User Equipment, Equipo de Usuario) obtenga el servicio proporcionado por la red de comunicación, el UE necesita obtener registro en el sistema por intermedio de un proceso de registro. La red, en función de la información proporcionada por el UE en el proceso de registro, ejercita el control del acceso para el UE, esto es, determina si el UE tiene los derechos para obtener registro en la red.

En la red existente, principalmente la red de acceso, en función de la liberación del equipo UE, determina qué modo de control del acceso se utilizará y determina los elementos de red en los que se pondrá en práctica el control del acceso. Actualmente, la red, en conformidad con la liberación del equipo UE, determina si el equipo UE tiene los derechos de obtención del registro en la red en dos modos. Un modo es: la red de acceso pone en práctica el control del acceso en el equipo UE de una versión antigua específica, pero la red central no pone en práctica ningún control del acceso en este equipo UE. A modo de ejemplo, la red de acceso utiliza un IMSI (Número de Identificador de Abonado Móvil Internacional, Identificador de Abonado Móvil Internacional) para poner en práctica el control del acceso en el UE que no soporta un CSG (Closed Subcriber Group, Grupo de Abonados Cerrado). El otro modo es: la red central pone en práctica el control del acceso en un nuevo equipo UE concreto, pero la red de acceso no pone en práctica ningún control del acceso sobre este equipo UE. A modo de ejemplo, la red central pone en práctica el control del acceso con CSG en el UE que soporta el CSG.

En la técnica relacionada, el equipo UE puede acceder a la red central directamente sin ningún control del acceso sobre el equipo UE, lo que menoscaba la seguridad de la red.

El artículo titulado “Control del acceso de legado y equipo CSG UE en la misma red” (ERICSSON, 3GPP DRAFT; R3-082907) da a conocer una solución de control del acceso de legado y CSG UE en la misma red.

El artículo titulado “Discusión sobre movilidad hacia el interior desde la célula marco 3G a HNB” (HUAWEI, 3GPP DRAFT; R3-090802) da a conocer una solución de una cuestión de control del acceso de UE durante el procedimiento de reubicación.

SUMARIO DE LA INVENCIÓN

Las formas de realización de la presente invención dan a conocer un sistema de comunicación según la reivindicación 12, una entidad de control del acceso según la reivindicación 9 y un método, según la reivindicación 1, para controlar el acceso de UE para garantizar la seguridad de la red.

Para cumplir dichos objetivos, formas de realización de la presente invención adoptan las soluciones técnicas siguientes:

Un método para controlar el acceso de UE dado a conocer en una forma de realización de la presente invención incluye:

la determinación, por una red de acceso, de un modo de control del acceso para un equipo UE, que depende del control del acceso puesta en práctica por una red central y

la puesta en práctica del control del acceso en el equipo UE cuando la red central no es capaz de poner en práctica el control del acceso en el equipo UE en el modo de control del acceso.

Una entidad de control del acceso dada a conocer en una forma de realización de la presente invención, incluye:

un primer módulo de recepción, configurado para recibir una demanda de acceso procedente de un equipo UE, que depende del control del acceso puesto en práctica por una red central;

un primer módulo de determinación, configurado para determinar si una red central capaz de poner en práctica el control del acceso puede seleccionarse para el UE y

un primer módulo de control del acceso, configurado para poner en práctica el control del acceso en el equipo UE si el primer módulo de determinación determina que ninguna red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE.

Un método para controlar el acceso del equipo UE dado a conocer en una forma de realización de la presente invención, incluye:

la determinación, por una red de acceso, de un modo de control del acceso para un equipo UE y

el envío de una demanda de conexión a una red central para iniciar la puesta en práctica por la red central de un control del acceso en el UE cuando la red central es capaz de poner en práctica el control del acceso en el UE en el modo de control del acceso.

Una entidad de control del acceso, dada a conocer en una forma de realización de la presente invención, incluye:

un segundo módulo de recepción, configurado para recibir una demanda de acceso desde un equipo UE que depende de un control del acceso puesto en práctica por una red central;

un segundo módulo de determinación, configurado para determinar si una red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE y

un segundo módulo de conexión, configurado para enviar una demanda de conexión a la red central si el segundo módulo de determinación determina que la red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE.

Un sistema de comunicación, que comprende un equipo de usuario, UE, una red de acceso y una primera red central, en donde,

la red de acceso está configurada para recibir una demanda de acceso procedente del UE que depende del control del acceso ejercido por una red central y poner en práctica el control del acceso en el equipo UE si ninguna red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE.

Por intermedio del sistema de comunicación, la entidad de control del acceso y el método para controlar el acceso de UE que se dan a conocer en formas de realización de la presente invención, la entidad de control del acceso de la red de acceso pone en práctica el control del acceso en el UE que depende del control del acceso puesto en práctica por la red central; o una red central capaz de poner en práctica el control del acceso en el UE se selecciona y se envía una demanda de conexión a la red central para iniciar la puesta en práctica por la red central del control del acceso. El control sobre el envío de la demanda de conexión puede impedir que el equipo UE se conecte a la red central que no pone en práctica el control del acceso en el UE. De este modo, antes de que el equipo UE acceda a la red central, el equipo UE se somete al control del acceso puesto en práctica por la red de acceso o la red central durante al menos un momento, lo que mejora la seguridad de la red.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama de flujo de un método para controlar el acceso de un equipo UE en una forma de realización de la presente invención,

La Figura 2 es un diagrama de flujo de un método para controlar el acceso de un equipo UE en una forma de realización de la presente invención,

La Figura 3 es un diagrama de flujo de un método para controlar el acceso de un equipo UE en una forma de realización de la presente invención;

La Figura 4 es un diagrama de flujo de un método para controlar el acceso de un equipo UE en una forma de realización de la presente invención;

La Figura 5 es un diagrama de flujo de un método para controlar el acceso de un equipo UE en una forma de realización de la presente invención;

La Figura 6 es un diagrama de flujo de un método para controlar el acceso de un equipo UE en una forma de realización de la presente invención;

La Figura 7 es un diagrama de flujo de un método para controlar el acceso de un equipo UE en una forma de realización de la presente invención;

La Figura 8 ilustra un diagrama estructural de un sistema de comunicación dado a conocer en una forma de

realización de la presente invención;

La Figura 9 ilustra un diagrama estructural de una entidad de control del acceso dada a conocer en una forma de realización de la presente invención;

La Figura 10 ilustra un diagrama estructural de un sistema de comunicación dado a conocer en una forma de realización de la presente invención y

La Figura 11 ilustra un diagrama estructural de una entidad de control del acceso dada a conocer en una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN DE LA INVENCIÓN

Un sistema de comunicación, una red de acceso y un método para controlar el acceso del equipo UE, que se dan a conocer en una forma de realización de la presente invención, se describe como sigue.

I. La red de acceso existente pone en práctica el control del acceso en el equipo UE de una versión específica. Este método puede estar relacionado con el control del acceso basado en IMSI. La entidad de control del acceso (tal como una estación base y/o pasarela) de la red de acceso memoriza los IMSIs de todos los equipos UEs que pueden pasar el control del acceso. El equipo UE envía el IMSI a la entidad de control del acceso durante el proceso de demanda de acceso. Si el equipo UE en la Lista IMSI Autorizada (una combinación de IMSIs memorizados en la entidad de control del acceso para la finalidad del control del acceso), la demanda de acceso procedente del UE se deja pasar; de no ser así, se rechaza la demanda de acceso procedente del UE.

II. Un HNB es privado y no está disponible para los usuarios externos sin el permiso del propietario. Desde la perspectiva del operador, la tarifa de la cobertura de HNB es inferior a la tarifa de la macro-red y el operador espera restringir al UE el uso de HNB. Por lo tanto, el HNB necesita soportar el control del acceso. Antes de enviar una demanda de acceso, el equipo UE necesaria incorporar un Grupo de Abonados Cerrado (CSG). La entidad de control del acceso memoriza los grupos CSGs de todos los equipos UEs que puedan pasar el control del acceso. El grupo CSG de la célula de HNB actual se envía a la entidad de control del acceso durante el proceso de demanda de acceso. Si los grupos de abonados incorporados por el UE de antemano incluyen el grupo CSG de la célula actual, se deja pasar la demanda de acceso procedente del UE; de no ser así, se rechaza la demanda de acceso procedente del equipo UE. Este modo de control del acceso surge con la emergencia del CSG. En general, una entidad de control de función (tal como SGSN (Serving GPRS Support Node, Nodo de soporte de GPRS de servicio)) en la red central pone en práctica el control del acceso en un equipo UE cuya versión soporta un CSG.

Actualmente, la red de acceso pone en práctica el control del acceso en un equipo UE cuya liberación no soporta un CSG, pero no pone en práctica el control del acceso en un UE cuya versión soporta un CSG. Sin embargo, con la emergencia del CSG, las redes centrales caen dentro de dos tipos: el primer tipo de red central no pone en práctica el control del acceso en el equipo UE y el segundo tipo pone en práctica el control del acceso en un equipo UE cuya versión soporta un CSG. En consecuencia, la red de acceso en la técnica anterior puede conectar un equipo UE cuya versión soporta un CSG en el primer tipo de red central sin ningún control del acceso y se dificulta la seguridad de la red de comunicación provista del primer tipo de red central de forma severa.

Las formas de realización de la presente invención dan a conocer un sistema de comunicación, una red de acceso y un método para controlar el acceso del UE para mejorar la seguridad de la red. El sistema de comunicación, la red central y el método para controlar el acceso del UE se describen, en detalle, haciendo referencia a los dibujos adjuntos. En las formas de realización de la presente invención, los equipos de usuario UEs pueden caer también en dos tipos. El primer tipo de equipos UEs depende del control del acceso puesto en práctica por la red de acceso y el segundo tipo depende del control del acceso puesto en práctica por la red central. A no ser que se especifique de otra manera, los equipos UE, en las formas de realización siguientes, se refieren a los equipos UE existentes que dependen del control del acceso ejercido por la red central. Se toma, a modo de ejemplo, un equipo UE cuya versión soporta un CSG.

Según se ilustra en la Figura 1, un método para controlar el acceso de UE en una forma de realización de la presente invención incluye las etapas siguientes:

S101. Recepción de una demanda de acceso procedente de un equipo UE que depende del control del acceso puesto en práctica por una red central.

S102. Poner en práctica el control del acceso en el equipo UE si ninguna red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE, en donde el control del acceso puede ponerse en práctica en función del Identificador de Abonado Móvil Internacional del equipo UE.

La demanda de acceso puede ser un mensaje de transmisión directa o un mensaje de configuración de conexión completa o un mensaje de demanda de acceso.

Después de que el equipo UE pase a través del control del acceso en S102, el UE envía una demanda de conexión del UE a la red central, con el fin de conectar el equipo UE en la red central que no pone en práctica el control del acceso en el UE. El control del acceso en la etapa S102 garantiza que el equipo UE se someta al control del acceso antes de que el equipo UE acceda a la red central, lo que mejora la seguridad de la red.

Cuando ninguna red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE en la etapa S102, los siguientes escenarios operativos son aplicables y difiere el control del acceso correspondiente. A continuación se describe el método, dado a conocer en una forma de realización de la presente invención, de controlar el acceso del equipo UE con referencia a escenarios operativos de aplicación detallados y los dibujos adjuntos.

Un sistema de comunicación incluye un equipo UE, una red de acceso y una red central. A modo de ejemplo, en las siguientes formas de realización, la función del control del acceso en la red central, se pone en práctica por un nodo SGSN. Una red de acceso puede incluir una estación base (HNB) y una pasarela (HNB GW).

Escenario operativo 1: La información de red central (incluyendo la información que indica si el control del acceso puede ponerse en práctica, o no, en el equipo UE que depende del control del acceso puesta en práctica por la red central) puede configurarse en la pasarela. Por lo tanto, después de que la red de acceso reciba una demanda de acceso procedente de un equipo UE que depende del control del acceso puesto en práctica por la red central, la pasarela es incapaz de seleccionar una red central que sea capaz de poner en práctica el control del acceso en el equipo UE en función de la información de red central configurada y entonces, la pasarela pone en práctica el control del acceso en el equipo UE.

Según se ilustra en la Figura 2, se incluyen las etapas siguientes.

S201. Antes de la comunicación con la red, el equipo UE necesita pasar el control del acceso. El equipo UE establece inicialmente una radioconexión con HNB. El proceso de control del acceso es bien conocido para los expertos en esta técnica y por ello, ya no se repite en esta descripción. El equipo UE puede notificar la información de versión del equipo UE a la red.

S202. El equipo UE envía la Unidad de Datos de Protocolos destinada para el nodo SGSN a HNB por intermedio de un mensaje de transmisión directa o un mensaje de configuración de conexión completa. Este mensaje puede incluir un IDNNS (Intra-Domain NAS Node Selector, Selector de Nodo NAS Intra-dominio) que el equipo UE necesita acceder inicialmente y un indicador de dominio, que facilita a la pasarela GW determinar la liberación de la red central que ha de accederse por el equipo UE y para decidir el método de control de la admisión.

S203. En función del contenido del mensaje recibido en la etapa S202, HNB comprueba la liberación del UE y conoce que el modo de control del acceso es la Lista CSG Autorizada (Allowed Close Subscriber Group List, Lista de Grupo de Abonados Cerrado Autorizada).

S204. Puesto que HNB no pone en práctica el control del acceso de la Lista CSG Autorizada, HNB envía una demanda de registro directamente a la pasarela HNB GW.

S205. La pasarela HNB GW, en función de la información de versión del equipo UE, determina seleccionar el nodo SGSN que es capaz de poner en práctica el control del acceso de la Lista CSG Autorizada para el UE. Puesto que ninguno de los nodos SGSNs, configurados por la pasarela HNB GW, es capaz de poner en práctica dicho tipo de control del acceso, la pasarela HNB GW, de forma opcional, pone en práctica el control del acceso en el UE, en función de la Lista IMSI Autorizada (Allowed International Mobile Subscriber Identity List, Lista de Identidades de Abonados Móviles Internacional Autorizada). Si se obtiene un éxito operativo, el procedimiento prosigue con la etapa S215; si falla, el procedimiento prosigue con la etapa S206.

S206. Si falla el control del acceso, o está ausente la información del UE (tal como IMSI), o la pasarela HNB GW no pone en práctica el control del acceso en este tipo de UE, la pasarela HNB GW reenvía un mensaje de rechazo de registro del UE o un mensaje de indicación de error al HNB. El mensaje puede incluir una indicación del modo para poner en práctica el control del acceso en el UE. Si HNB necesita poner en práctica el control del acceso, pero la información memorizada (a modo de ejemplo, para falta IMSI) es deficiente para el control del acceso, el procedimiento prosigue con la etapa S207.

S207. HNB inicia un procedimiento de obtención de la información del UE y envía una demanda de información al equipo UE.

S208. El equipo UE reenvía la información demandada (tal como IMSI) a HNB en función del contenido demandado.

S209. HNB obtiene información del UE y de forma opcional, pone en práctica el control del acceso sobre el UE, en función de la Lista IMSI Autorizada. Si falla el control del acceso, el procedimiento prosigue con la etapa S213. Si HNB no pone en práctica el control del acceso o el control del acceso tiene éxito operativo, el procedimiento

prosigue con la etapa S210.

S210. HNB envía una demanda de registro a la pasarela HNB GW.

S211. La pasarela HNB GW pone en práctica el control del acceso de la Lista IMSI Autorizada en el UE en función de la información del UE obtenida (tal como IMSI, información de versión). Si el UE falla en el acceso a la pasarela HNB GW, el procedimiento prosigue con la etapa S212; si el acceso tiene éxito operativo, el procedimiento prosigue con la etapa S215.

S212. La pasarela HNB GW inicia un proceso de eliminación de registro del UE para HNB.

S213. Después de recibir un mensaje de eliminación de registro desde la pasarela HNB GW, HNB inicia un proceso de fallo de acceso para el UE por intermedio de una interfaz de aire.

S214. El recurso de radioconexión de la interfaz de aire está liberado.

S215. La pasarela HNB GW reenvía un mensaje de aceptación de registro a HNB.

S216. HNB envía una demanda de conexión a la pasarela HNB GW después de recibir el mensaje de aceptación de registro.

S217. La pasarela HNB GW sigue enviando una nueva demanda de conexión al nodo SGSN.

S218. El nodo SGSN reenvía un mensaje de confirmación de conexión a la pasarela HNB GW y el equipo UE accede a la red de forma operativamente satisfactoria.

S219. Se realizan otros procedimientos no de acceso.

Escenario operativo 2:

A diferencia con el primer escenario operativo antes descrito, este escenario operativo tiene información de red central configurada en HNB. Cuando HNB, en función de la información de red central configurada, tiene conocimiento de que ninguna red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE, HNB pone en práctica el control del acceso directamente en el equipo UE.

Según se ilustra en la Figura 3, que incluye las etapas siguientes:

S301. El equipo UE establece una radioconexión con HNB.

S302. El equipo UE envía la PDU para el nodo SGSN a HNB a través de un mensaje de transmisión directa o un mensaje de configuración de conexión completa. Este mensaje puede incluir un IDNNS que el UE necesita para acceder inicialmente y puede incluir un indicador de dominio, lo que facilita a la pasarela GW determinar la liberación de la red central objeto de acceso por el UE y para decidir el método del control del acceso.

S303. En función del contenido del mensaje recibido en la etapa S302, HNB comprueba la liberación del equipo UE y conoce que el modo de control del acceso es la Lista CSG Autorizada.

S304. Puesto que HNB no pone en práctica el control del acceso en función de la Lista CSG Autorizada y HNB ha configurado la información de liberación de la red central, HNB, de forma opcional, pone en práctica el control del acceso, en función de Lista IMSI Autorizada, en el equipo UE, si la red central correspondiente a HNB no soporta el control del acceso en función de la Lista CSG Autorizada. Si la información del control del acceso es deficiente (a modo de ejemplo, por falta de IMSI), HNB envía un mensaje de demanda de información al equipo UE o rechaza directamente la demanda de acceso y el procedimiento prosigue con la etapa S310.

S305. El equipo UE reenvía la información demandada (tal como IMSI) a HNB en función del contenido demandado.

S306. HNB obtiene información de UE y, de forma opcional, pone en práctica el control del acceso en el UE en función de la Lista IMSI Autorizada. Si falla el control del acceso, el procedimiento prosigue con la etapa S310.

S307. Si HNB no pone en práctica el control del acceso o el control del acceso tiene éxito operativo, HNB envía una demanda de registro a la pasarela HNB GW.

S308. La pasarela HNB GW pone en práctica el control del acceso, en función de la Lista IMSI Autorizada, en el equipo UE en función de la información de UE obtenida (tal como: IMSI, información de liberación). Si el equipo UE falla en el acceso a la pasarela HNB GW, el procedimiento prosigue con la etapa S309; si el acceso tiene éxito operativo, el procedimiento prosigue con la etapa S312.

S309. La pasarela HNB GW inicia un proceso de eliminación del registro de UE para HNB.

S310. Después de recibir un mensaje de eliminación de registro desde la pasarela HNB GW, HNB inicia un proceso de fallo del acceso al UE por intermedio de una interfaz de aire.

S311. Se libera el recurso de radioconexión de la interfaz de aire.

S312. Si tiene éxito operativo el control del acceso en la etapa S308, la pasarela HNB GW reenvía un mensaje de aceptación de registro a HNB.

S313. HNB envía una demanda de conexión a la pasarela HNB GW después de recibir el mensaje de aceptación de registro.

S314. La pasarela HNB GW sigue enviando una demanda de conexión al nodo SGSN de nuevo.

S315. El nodo SGSN reenvía un mensaje de confirmación de conexión a la pasarela HNB GW y el equipo UE accede a la red de forma operativamente satisfactoria.

S316. Se realizan otros procedimientos no de acceso.

En este escenario operativo, la estación base está configurada para recibir una demanda de acceso desde el UE que depende del control del acceso puesto en práctica por la red central y pone en práctica el control del acceso en el UE después de conocer que la red central disponible no pone en práctica el control del acceso en el UE. Después de que el equipo UE pase el control del acceso puesto en práctica por la estación base, la pasarela envía una demanda de conexión a la red central, con el fin de hacer que el equipo UE acceda a la red central. La demanda de conexión no incluye información que no pueda identificarse por la red central.

Escenario operativo 3:

La red de acceso no configura la información de red central (la información incluye si el control del acceso puede ponerse en práctica, o no, en el equipo UE), pero la red central puede establecer la política de acceso y analizar, en función de dicha política, la demanda de conexión, enviada por la red de acceso, del equipo UE, que depende del control del acceso puesto en práctica por la red central y entrega un mensaje de fallo de acceso a la red de acceso en función de la demanda de conexión y la red de acceso, en función del mensaje de fallo del acceso, determina que la red central es incapaz de poner en práctica el control del acceso en el equipo UE. Es decir, se establecen políticas de acceso en la red central y la red central lo notifica a la red de acceso para poner en práctica el control del acceso en el equipo UE (las políticas de acceso no son equivalentes al control del acceso. La red central es incapaz de poner en práctica el control del acceso en el equipo UE, pero puede simplemente analizar el mensaje informado por la red de acceso).

Según se ilustra en la Figura 4, se incluyen las etapas siguientes:

S401. El equipo UE establece una radioconexión con HNB.

S402. El equipo UE envía la PDU destinada para el nodo SGSN a HNB por intermedio de un mensaje de transmisión directa o un mensaje de configuración de conexión completa. Este mensaje puede incluir un IDNNS que el UE necesita para el acceso inicial y un indicador de dominio, que facilita a la pasarela GW la determinación de la liberación de la red central para su acceso por el equipo UE y para decidir el método de control de admisión.

S403. En función del contenido del mensaje recibido en S402, HNB comprueba la liberación del equipo UE y conoce que el modo del control del acceso es la Lista CSG Autorizada.

S404. Puesto que HNB no pone en práctica el control del acceso según la Lista CSG Autorizada, HNB envía una demanda de registro a la pasarela HNB GW directamente.

S405. La pasarela HNB GW envía un identificador de contexto, que se asigna al UE, al HNB por intermedio de un mensaje de aceptación de registro.

S406. HNB envía un mensaje de conexión que incluye un identificador CSG ID a la pasarela HNB GW.

S407. Puesto que la pasarela HNB GW no pone en práctica el control del acceso según la Lista CSG Autorizada, la pasarela HNB GW envía una demanda de conexión al nodo SGSN. El mensaje de demanda incluye el identificador CSG ID de la célula objeto de acceso por el equipo UE.

S408. El nodo SGSN reenvía un mensaje de confirmación de conexión a la pasarela HNB GW.

S409. Se establece una política en el nodo SGSN: si el nodo SGSN de esta liberación no soporta el control del acceso baso en CSG o es incapaz de identificar el elemento de información (IE) del CSG ID en el mensaje, el nodo SGSN inicia un proceso de gestión excepcional. En consecuencia, el nodo SGSN envía un proceso de gestión excepcional y rechaza el acceso del equipo UE.

S410. El nodo SGSN reenvía un mensaje de fallo del acceso a la pasarela HNB GW. El mensaje incluye la causa del fallo (no soporte del control del acceso basado en CSG o incapacidad de identificar el elemento de información). De forma opcional, el mensaje incluye el identificador y el contenido del IE que causa el fallo. En función de la información de excepción, la pasarela HNB GW conoce que el nodo SGSN no soporta el modo de control del acceso basado en la Lista CSG Autorizada.

S411. De forma opcional, la pasarela HNB GW pone en práctica el control del acceso, en función de la Lista IMSI Autorizada, en el equipo UE y el procedimiento prosigue con la etapa S412. Si la pasarela HNB GW pone en práctica el control del acceso en el equipo UE, el procedimiento prosigue con la etapa S417.

S412. Si la pasarela HNB GW necesita poner en práctica el control del acceso y la información memorizada (a modo de ejemplo, para falta de IMSI) es deficiente para el control del acceso, la pasarela HNB GW inicia un procedimiento de obtención de la información de UE y envía una demanda de información a HNB.

S413. HNB recibe la demanda de información desde la pasarela HNB GW y envía una demanda de información al UE en función del contenido demandado.

S414. El UE reenvía la información demandada (tal como IMSI) a HNB en función del contenido demandado.

S415. HNB envía la información del UE obtenida a la pasarela HNB GW.

S416. La pasarela HNB GW pone en práctica el control del acceso, en función de la Lista IMSI Autorizada, en el equipo UE en función de la información de UE obtenida (tal como IMSI). Si el equipo UE falla en el acceso a la pasarela HNB GW, el procedimiento prosigue con la etapa S417; si el control del acceso tiene éxito operativo, el procedimiento prosigue con la etapa S420.

S417. La pasarela HNB GW inicia un proceso de eliminación de registro de UE para HNB.

S418. Después de recibir un mensaje de alimentación de registro de procedente de la pasarela HNB GW, HNB inicia un proceso de fallo de acceso para el UE por intermedio de una interfaz de aire.

S419. El recurso de radioconexión de la interfaz de aire se libera.

S420. Si tiene éxito operativo el control del acceso en la etapa S416 y se libera la conexión del UE entre la pasarela HNB GW y el nodo SGSN, la pasarela HNB GW envía una nueva demanda de conexión al nodo SGSN. La nueva demanda de conexión no incluye información que no pueda identificarse por la red central (tal como CSG ID).

S421. Si la conexión entre la pasarela HNB GW y el nodo SGSN se establece de nuevo, el nodo SGSN reenvía un mensaje de confirmación de conexión a la pasarela HNB GW.

S422. Se realizan otros procedimientos no de acceso.

En la Figura 4, a través de la etapa S412, la pasarela HNB GW inicia un procedimiento de obtención de información en función del control del acceso local. Este procedimiento puede iniciarse también por HNB. Según se ilustra en la Figura 5, se incluyen las etapas siguientes:

Las etapas S501-S511 son las mismas que S401-S411 y por ello no se repiten en esta descripción.

S512. Si la información del UE requerida para el control del acceso es deficiente (a modo de ejemplo, por falta de IMSI) o no se pone en práctica el control del acceso, la pasarela HNB GW envía un mensaje de eliminación de registro del UE a HNB directamente. Este mensaje puede incluir una indicación del modo para poner en práctica el control del acceso en el equipo UE.

S513. Si HNB necesita poner en práctica el control del acceso y la información memorizada (a modo de ejemplo, por falta de IMSI) es deficiente para el control del acceso, HNB inicia un procedimiento de obtención de la información del UE y envía una demanda de información al UE. Si HNB no pone en práctica el control del acceso o el control del acceso tiene éxito operativo, el procedimiento prosigue con la etapa S516.

S514. El equipo UE reenvía la información demandada (tal como IMSI) a HNB en función del contenido demandado.

S515. HNB obtiene la información del UE y de forma opcional, pone en práctica el control del acceso en el equipo

UE, en función de la Lista IMSI Autorizada. Si falla el control del acceso, el procedimiento prosigue con la etapa S519.

S516. HNB envía una demanda de registro a la pasarela HNB GW.

S517. La pasarela HNB GW pone en práctica el control del acceso de la Lista IMSI Autorizada en el equipo UE en función de la información de UE obtenida (tal como: IMSI, información de liberación). Si el equipo UE falla en el acceso a la pasarela HNB GW, el procedimiento prosigue con la etapa S518; si el acceso tiene éxito operativo, el procedimiento prosigue con la etapa S512.

S518. La pasarela HNB GW inicia un proceso de eliminación de registro del UE para HNB.

S519. Después de recibir un mensaje de eliminación de registro desde la pasarela HNB GW, HNB inicia un proceso de fallo de acceso al UE por intermedio de una interfaz de aire.

S520. El recurso de radioconexión de la interfaz de aire está liberado.

S521. Si el control del acceso en la etapa S517 tiene éxito operativo, la pasarela HNB GW reenvía un mensaje de aceptación de registro a HNB.

S522. HNB envía una demanda de conexión a la pasarela HNB GW después de recibir el mensaje de aceptación de registro.

S523. La pasarela HNB GW sigue enviando una nueva demanda de conexión al nodo SGSN.

S524. El nodo SGSN reenvía un mensaje de confirmación de conexión a la pasarela GW y el equipo UE accede a la red de forma operativamente satisfactoria.

S525. Se realizan otros procedimientos no de acceso.

En el escenario operativo ilustrado en la Figura 4 y en la Figura 5, si ninguna red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE, el control del acceso se pone en práctica en el UE como sigue:

La red de acceso selecciona una red central y envía una demanda de conexión a la red central, en donde la demanda de conexión incluye información que no puede identificarse por la red central;

La red de acceso recibe un mensaje de fallo del acceso reenviado por la red central para fallo de identificación de la información;

La red de acceso, en función del mensaje de fallo del acceso, determina que la red central es incapaz de poner en práctica el control del acceso en el equipo UE y

La red de acceso pone en práctica el control del acceso en el UE.

En las formas de realización antes descritas, después de que el UE pase el control del acceso puesto en práctica por la red de acceso, la red de acceso envía una demanda de conexión a la red central incapaz de poner en práctica el control del acceso en el equipo UE, en donde la demanda de conexión enviada no incluye información que no pueda identificarse por la red central.

Según se ilustra en la Figura 6, otro método para controlar el acceso del equipo UE en una forma de realización de la presente invención, incluye las etapas siguientes:

S601. Recibir una demanda de acceso desde un equipo UE que depende del control del acceso puesto en práctica por una red central.

S602. Enviar una demanda de conexión a la red central si una red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE.

La demanda de acceso puede ser un mensaje de transmisión directa o un mensaje de configuración de conexión completa o un mensaje de demanda de acceso.

En esta forma de realización, una red central capaz de poner en práctica el control del acceso en el equipo UE se selecciona al respecto y una demanda de conexión se envía a la red central para iniciar la puesta en práctica por la red central del control del acceso. El control sobre el envío de la demanda de conexión, con el fin de impedir al equipo UE que se conecta a la red central que no ponga en práctica el control del acceso en el equipo UE. De este

modo, antes de que el equipo UE acceda a la red central, el equipo UE se somete al control del acceso puesto en práctica por la red central, lo que mejora la seguridad de la red.

A continuación se describe esta forma de realización, en detalle, haciendo referencia a un escenario operativo de aplicación específico.

Según se ilustra en la Figura 7, se incluyen las etapas siguientes:

S701. El equipo UE establece una conexión de RRC con HNB y comunica información tal como ID (ID temporal o IMSI), con la liberación del UE.

S702. Por intermedio de la radioconexión, el equipo UE envía un mensaje de demanda de acceso a HNB. El mensaje puede incluir un IDNNS que el UE necesita para acceder inicialmente y un indicador de dominio, que facilita a la pasarela GW determinar la liberación de la red central objeto de acceso por el UE y para decidir el método de control de admisión.

S703. HNB determina la Lista CSG Autorizada como el modo de control del acceso en función de la información del UE y no pone en práctica el control del acceso en el equipo UE.

S704. HNB envía un mensaje de registro de UE (el mensaje puede incluir IMSI, UE Rel, UE Cap) a la pasarela HNB GW.

S705. En función de la información del UE, la pasarela HNB GW determina que el modo de control del acceso es el modo de la Lista CSG Autorizada. La pasarela HNB GW no pone en práctica el control del acceso en el equipo UE, pero permite siempre el acceso del UE.

S706. La pasarela HNB GW reenvía un mensaje de aceptación de registro del UE a HNB.

S707. Después de recibir el mensaje de aceptación, HNB envía un mensaje de conexión a la pasarela HNB GW. El mensaje de conexión incluye un CSG ID de la célula objeto de acceso por el UE.

S708. La pasarela HNB GW, en función de la información de configuración del nodo SGSN pertinente, selecciona un nodo SGSN capaz de poner en práctica el control del acceso, sobre la base de la Lista CSG Autorizada, en el equipo UE actual.

S709. La pasarela HNB GW envía un mensaje de demanda de conexión a la red central. El mensaje de demanda de conexión incluye un CSG ID de la célula objeto de acceso por el equipo UE.

S710. El nodo de la red central reenvía un mensaje de confirmación de conexión a la pasarela HNB GW.

S711. De modo opcional, continúan otros procedimientos de señales de gestión móviles.

S712. El nodo de la red central pone en práctica el control del acceso en el equipo UE en función del identificador CSG ID recibido en S708.

S713. Continuar el procedimiento de señalización de NAS.

En las formas de realización anteriores, la red de acceso incluye una estación base y una pasarela. Es precisamente la estación base o la pasarela la que pone en práctica el control del acceso en el UE o, después de que la estación base ponga en práctica el control del acceso en el UE por primera vez, la pasarela pone en práctica el control del acceso en el UE por segunda vez. De forma alternativa, la pasarela envía una instrucción a la estación base para poner en práctica el control del acceso en el equipo UE, en donde la instrucción incluye un modo de control del acceso. A modo de ejemplo, la pasarela da instrucciones a la estación base para poner en práctica el control del acceso en el equipo UE en el proceso de registro de la estación base. El procedimiento incluye las etapas siguientes (no ilustradas):

Etapa 1: La pasarela recibe una demanda de registro desde la estación base.

Etapa 2: La pasarela reenvía un mensaje de aceptación de registro a la estación base. El mensaje de aceptación de registro incluye el modo de control del acceso para el equipo UE que depende del control del acceso puesto en práctica por la red central.

Un sistema de comunicación y una entidad de control del acceso se dan a conocer en una forma de realización de la presente invención.

Según se ilustra en la Figura 8, el sistema de comunicación incluye un equipo UE1, una red de acceso 3 y una red

central 5.

La red de acceso 3 está configurada para recibir una demanda de acceso desde el equipo UE1 que depende del control del acceso puesto en práctica por la red central 5 y para poner en práctica el control del acceso en el equipo UE1 si una red central 5 capaz de poner en práctica el control del acceso no puede seleccionarse para el equipo UE1. Después de que el equipo UE1 pasa el control del acceso puesto en práctica por la red de acceso 3, la red de acceso 3 envía una demanda de conexión a la red central 5.

En este sistema, la red central 5 puede configurarse, además, para establecer una política de acceso para el equipo UE1 que depende del control del acceso puesto en práctica por la red central 5; para determinar, en conformidad con la política de acceso, si una demanda de acceso incluye información que no puede identificarse localmente cuando se recibe la demanda de conexión enviada por la red de acceso 3 y si la demanda de acceso incluye información que no puede identificarse, para reenviar un mensaje de fallo de acceso a la red de acceso 3, en donde la red de acceso 3, en función del mensaje de fallo del acceso, conoce que la red central 5 capaz de poner en práctica el control del acceso en el equipo UE1 no puede seleccionarse y la red de acceso 3 pone en práctica el control del acceso en el equipo UE1. Después de que el equipo UE1 pase el control del acceso puesto en práctica por la red de acceso 3, la red de acceso 3 envía una demanda de conexión a la red central 5, en donde la demanda de conexión no incluye información que no pueda identificarse por la red central.

Según se ilustra en la Figura 9, se da a conocer una entidad de control del acceso. La entidad de control del acceso puede ser una estación base o una pasarela en la red de acceso. La entidad de control del acceso incluye:

un primer módulo de recepción 31, configurado para recibir una demanda de acceso desde un equipo UE que depende del control del acceso puesto en práctica por una red central;

un primer módulo de determinación 32, configurado para determinar si una red central capaz de poner en práctica el control del acceso puede seleccionarse, o no, para el equipo UE y

un primer módulo de control del acceso 33, configurado para poner en práctica el control del acceso en el equipo UE si el primer módulo de determinación 32 que determina que ninguna red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE.

La entidad de control del acceso puede incluir, además:

un primer módulo de configuración 34, configurado para poder configurar la información de red central como una base para que el primer modo de determinación 32 pueda determinar si una red central capaz de poner en práctica el control del acceso puede seleccionarse, o no, para el equipo UE.

El primer módulo de determinación 32 está configurado, además, para determinar, en función del mensaje de fallo del acceso de la red central, que ninguna red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE. El primer módulo de determinación 32 puede incluir, además:

una primera unidad de selección 321, configurada para: seleccionar una red central que no requiera el control del acceso para el equipo UE si el primer módulo de determinación 32 no puede seleccionar una red central capaz de poner en práctica el control del acceso para el equipo UE y para enviar una demanda de conexión a la red central, en donde la demanda de conexión incluye información que no puede identificarse por la red central.

Una primera unidad de realimentación operativa 322, configurada para recibir un mensaje de fallo del acceso realimentado por la red central seleccionada por la primera unidad de selección 321 y para dar instrucciones a la primera unidad de control del acceso 33 para poner en práctica el control del acceso en el equipo UE.

En correspondencia con la forma de realización del método, la entidad de control del acceso puede ser una estación base o una pasarela. La estación base está configurada, además, para enviar su propia demanda de registro a la pasarela. Después de recibir la demanda de registro enviada por la estación base, la pasarela puede reenviar un mensaje de aceptación de registro a la estación base, en donde el mensaje de aceptación de registro indica el modo de control del acceso puesto en práctica por la estación base para el equipo UE (incluyendo el UE que depende del control del acceso puesto en práctica por la red central). De este modo, la estación base puede procesar, en correspondencia, el equipo UE que depende del control del acceso puesto en práctica por la red central en función del modo de control del acceso indicado por la pasarela. El procedimiento de procesamiento es similar al escenario operativo ilustrado en la Figura 2 y por ello no se describe aquí en detalle. El procedimiento puede reducir los mensajes que han de reenviarse y transmitir mensajes de forma transparente en el proceso del control del acceso, puesto en práctica por la red de acceso, en el equipo UE.

Con el sistema de comunicación y la entidad de control del acceso en esta forma de realización, la entidad de control del acceso, tal como una estación base o una pasarela en la red de acceso 3, pone en práctica el control del acceso en el equipo UE1 que depende del control del acceso de la red central 5, con el fin de mejorar la seguridad de la red.

Un sistema de comunicación y una entidad de control del acceso se dan a conocer en otra forma de realización de la presente invención.

Según se ilustra en la Figura 10, el sistema incluye un equipo UE2, una red de acceso 4 y una red central 6.

La red de acceso 4 está configurada para recibir una demanda de acceso desde el equipo UE2 que depende del control del acceso puesto en práctica por la red central 6 y para enviar una demanda de conexión a la red central 6 si una red central 6 capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE2.

En correspondencia con el sistema, la entidad de control del acceso de la red de acceso puede ser una pasarela. Según se ilustra en la Figura 11, la entidad de control del acceso incluye:

un segundo módulo de recepción 41, configurado para recibir una demanda de acceso desde un equipo UE que depende del control del acceso puesto en práctica por una red central;

un segundo módulo de determinación 42, configurado para determinar si una red central capaz de poner en práctica el control del acceso puede seleccionarse, o no, para el equipo UE y

un segundo módulo de conexión 43, configurado para enviar una demanda de conexión a la red central si el segundo módulo de determinación 42 determina que la red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE.

El segundo módulo de configuración 44 está configurado para poder establecer la configuración de la información de red central que indica la capacidad de puesta en práctica del control del acceso en el equipo UE y sirve como una base para que el segundo módulo de determinación 42 pueda determinar si una red central capaz de poner en práctica el control del acceso puede seleccionarse, o no, para el equipo UE.

Con el sistema de comunicación y la entidad de control del acceso que se dan a conocer en esta forma de realización, una red central 6 capaz de poner en práctica el control del acceso en el equipo UE2 se selecciona al respecto y se envía una demanda de conexión a la red central 6 para iniciar la red central 6 en la puesta en práctica del control del acceso. El control sobre el envío de la demanda de conexión, con el fin de impedir la conexión de UE2 a la red central 6 que no pone en práctica el control del acceso en el equipo UE2. De este modo, antes de que el equipo UE2 acceda a la red central, el equipo UE2 se somete a un control del acceso puesto en práctica por la red central, lo que mejora la seguridad de la red.

Los expertos en esta técnica deben entender que la totalidad o parte de las etapas del método dado a conocer en las formas de realización anteriores puede ponerse en práctica por un programa que proporciona instrucciones al hardware pertinente. El programa informativo puede memorizarse en un medio de almacenamiento legible por ordenador. Cuando se ejecuta el programa informático, el programa realiza las etapas del método especificado en cualquier forma de realización anterior. El medio de almacenamiento puede ser un disco magnético, un CD-ROM, una memoria de lectura solamente (ROM) o una memoria de acceso aleatorio (RAM).

Las anteriores descripciones son simplemente formas de realización, a modo de ejemplo, de la presente invención, pero no pretenden limitar el alcance de protección de la presente invención. Cualesquiera modificaciones, variaciones o sustituciones que puedan derivarse fácilmente por los expertos en esta técnica caerán dentro del alcance de protección de la presente invención. Por lo tanto, el alcance de protección de la presente invención está supeditado a lo que se estipula en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para controlar el acceso de un equipo de usuario, UE, que comprende:

la determinación, por una red de acceso, de un modo de control del acceso para un equipo UE, que depende de un control del acceso puesto en práctica por una red central y caracterizado por cuanto que:

la puesta en práctica, por la red de acceso, del control del acceso en el equipo UE cuando la red central es incapaz de ejercer el control del acceso en el equipo UE en el modo de control del acceso.

2. El método según la reivindicación 1, en donde: el modo de control del acceso para el equipo UE es un modo de lista de Grupo de Abonados Cerrados Autorizada o una Lista CSG Autorizada;

la puesta en práctica de un control del acceso en el equipo UE cuando la red central es incapaz de ejercer el control del acceso en el equipo UE en el modo de control del acceso comprende:

la puesta en práctica, por la red de acceso, del control del acceso en el equipo UE en un modo de Lista de Identificadores de Abonados Móviles Internacionales Autorizada o Lista IMSI Autorizada, cuando la red de acceso determina que la red central es incapaz de poner en práctica el control del acceso en el equipo UE en el modo de Lista CSG Autorizada.

3. El método según la reivindicación 2, en donde: la información de red central está configurada en una pasarela de la red de acceso o está configurada en una estación base de la red de acceso; la información de red central comprende información que indica si el control del acceso puede ponerse en práctica, o no, en el equipo UE que depende del control del acceso ejercido por la red central;

la determinación de que la red central es incapaz de poner en práctica el control del acceso en el equipo UE, en el modo de Lista de CSG Autorizada, comprende:

la determinación, por la pasarela de la red de acceso, de que la red central es incapaz de poner en práctica el control del acceso en el UE en el modo de Lista CSG Autorizada en función de la información de red central configurada en la pasarela;

o comprende:

la determinación, por la estación base de la red de acceso, de que la red central es incapaz de poner en práctica el control del acceso en el UE en el modo de Lista CSG Autorizada en función de la información de red central configurada en la estación base.

4. El método según la reivindicación 1, en donde: la determinación de que la red central es incapaz de poner en práctica el control del acceso en el UE en el modo de control del acceso comprende:

el envío, por una pasarela de la red de acceso, de una demanda de conexión a la red central, en donde la demanda de conexión incluye un identificador CSG ID de una célula objeto de acceso por el equipo UE;

la recepción de un mensaje de fallo de acceso desde la red central;

la determinación de que la red central es incapaz de poner en práctica el control del acceso en el equipo UE en el modo de control del acceso en función del mensaje de fallo de acceso.

5. El método según cualquiera de las reivindicaciones 1 a 4, en donde: la determinación, por una red de acceso, de un modo de control del acceso para el equipo UE comprende:

la recepción, por una pasarela de la red de acceso, de una demanda de registro, en donde la demanda de registro se envía por una estación base después de que la estación base reciba una demanda de acceso desde el equipo UE y

el conocimiento aprendido, por la pasarela en función de la demanda de registro, de que el equipo UE depende del control del acceso puesto en práctica por la red central y la determinación de un modo de control del acceso para el equipo UE;

o que comprende:

la recepción, por una estación base de la red de acceso, de una demanda de acceso procedente del equipo UE y

el conocimiento por aprendizaje, por la estación base, de que el equipo UE depende del control del acceso puesto

en práctica por la red central y la determinación de un modo de control del acceso para el equipo UE, en función de la demanda de acceso procedente del UE.

6. El método según la reivindicación 1, en donde: la puesta en práctica del control del acceso en el equipo UE comprende:

poner en práctica, por la red de acceso, el control del acceso en el equipo UE en conformidad con un Identificador de Abonado Móvil Internacional del UE.

7. El método según la reivindicación 1, en donde:

la puesta en práctica, por una pasarela de la red de acceso, del control del acceso en el UE y

después de la puesta en práctica, por una pasarela de la red de acceso, el control del acceso en el UE, el método comprende, además:

el envío, por la pasarela, de un mensaje a una estación base de la red de acceso, incluyendo dicho mensaje una indicación de un modo para poner en práctica el control del acceso en el equipo UE, cuando la pasarela pone en práctica el control del acceso en el UE de forma operativa no satisfactoria.

8. El método según la reivindicación 7, en donde, después del envío del mensaje a la estación base de la red de acceso, el método comprende, además:

la recepción, por la pasarela, de una demanda de registro reenviada por la estación base, en donde la demanda de registro incluye un Identificador de Abonado Móvil Internacional del UE y se envía después de que la estación base ponga en práctica el control del acceso de forma satisfactoria o la estación base no ponga en práctica ningún control del acceso;

la obtención, por la pasarela, del Identificador de Abonado Móvil Internacional y

la puesta en práctica, por la pasarela, del control del acceso sobre el equipo UE en función del Identificador de Abonado Móvil Internacional.

9. Una entidad de control del acceso que comprende:

un primer módulo de recepción (31), configurado para recibir una demanda de acceso desde un equipo de usuario, UE, que depende del control del acceso ejercido por una red central y caracterizado por cuanto que:

un primer módulo de determinación (32), configurado para determinar si cualquier red central capaz de poner en práctica el control del acceso, puede seleccionarse para el UE y

un primer módulo de control del acceso (33), configurado para poner en práctica el control del acceso en el UE si el primer módulo de determinación (32) determina que ninguna red central capaz de poner en práctica el control del acceso, puede seleccionarse para el equipo UE.

10. La entidad de control del acceso según la reivindicación 9 que comprende, además:

un primer módulo de configuración (34), configurado para poder configurar la información de red central como una base para el primer módulo de determinación (32) para determinar si cualquier red central capaz de poner en práctica el control del acceso puede seleccionarse para el equipo UE.

11. La entidad de control del acceso según la reivindicación 9 o 10, en donde el primer módulo de determinación (32) comprende, además:

una primera unidad de selección (321), configurada para: seleccionar una red central que no requiera control del acceso para el equipo UE si el primer módulo de determinación (32) determina que ninguna red central capaz de poner en práctica el control del acceso, puede seleccionarse para el equipo UE y enviar una demanda de conexión a la red central, en donde la demanda de conexión incluye información que no puede identificarse por la red central y

una primera unidad de realimentación operativa (322), configurada para recibir un mensaje de fallo de acceso realimentado por la red central seleccionada por la primera unidad de selección (321) y para dar instrucciones al primer módulo de control del acceso (33) para poner en práctica el control del acceso en el UE.

12. Un sistema de comunicación, que comprende un equipo de usuario, UE, una red de acceso y una primera red central, caracterizado por cuanto que:

la red de acceso que se está configurando para recibir una demanda de acceso procedente del UE, que depende del control del acceso puesto en práctica por una red central y la puesta en práctica del control del acceso en el equipo UE si ninguna red central, que es capaz de poner en práctica el control del acceso, puede seleccionarse para el equipo UE.

13. El sistema de comunicación según la reivindicación 12, en donde la red de acceso está configurada, además, para enviar una demanda de conexión a la primera red central después de que el equipo UE pase el control del acceso puesto en práctica por la red de acceso.

14. El sistema de comunicación según la reivindicación 13,

en donde la primera red central está configurada para establecer una regla de acceso para el equipo UE que depende del control del acceso puesto en práctica por la red central y para determinar, en función de la regla de acceso, si una demanda de acceso incluye información que no pueda identificarse, al nivel local, cuando se reciba la demanda de conexión enviada por la red de acceso y si la demanda de acceso incluye información que no puede identificarse, reenviar un mensaje de fallo de acceso a la red de acceso;

en donde la demanda de conexión no incluye la información que no puede identificarse por la red central.

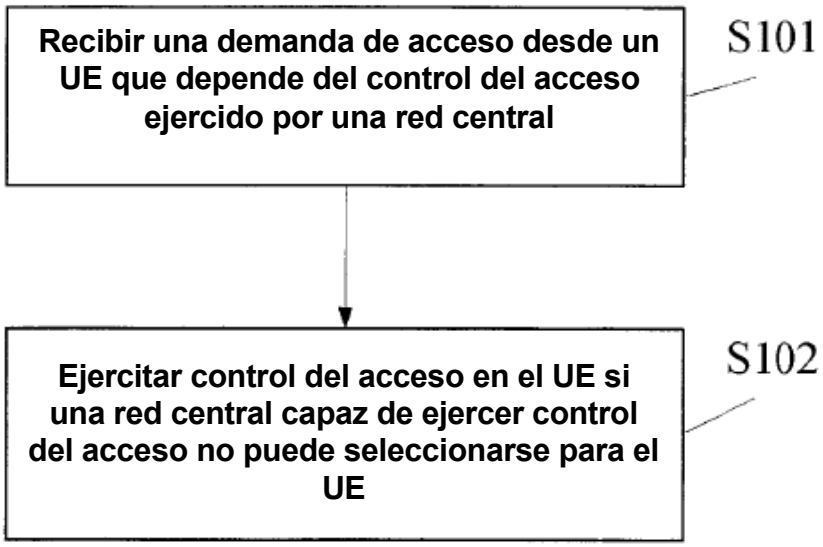
Recibir una demanda de acceso desde un UE que depende del control del acceso ejercido por una red central
S101
Ejercitar control del acceso en el UE si una red central capaz de ejercer control del acceso no puede seleccionarse para el UE
S102

FIG. 1

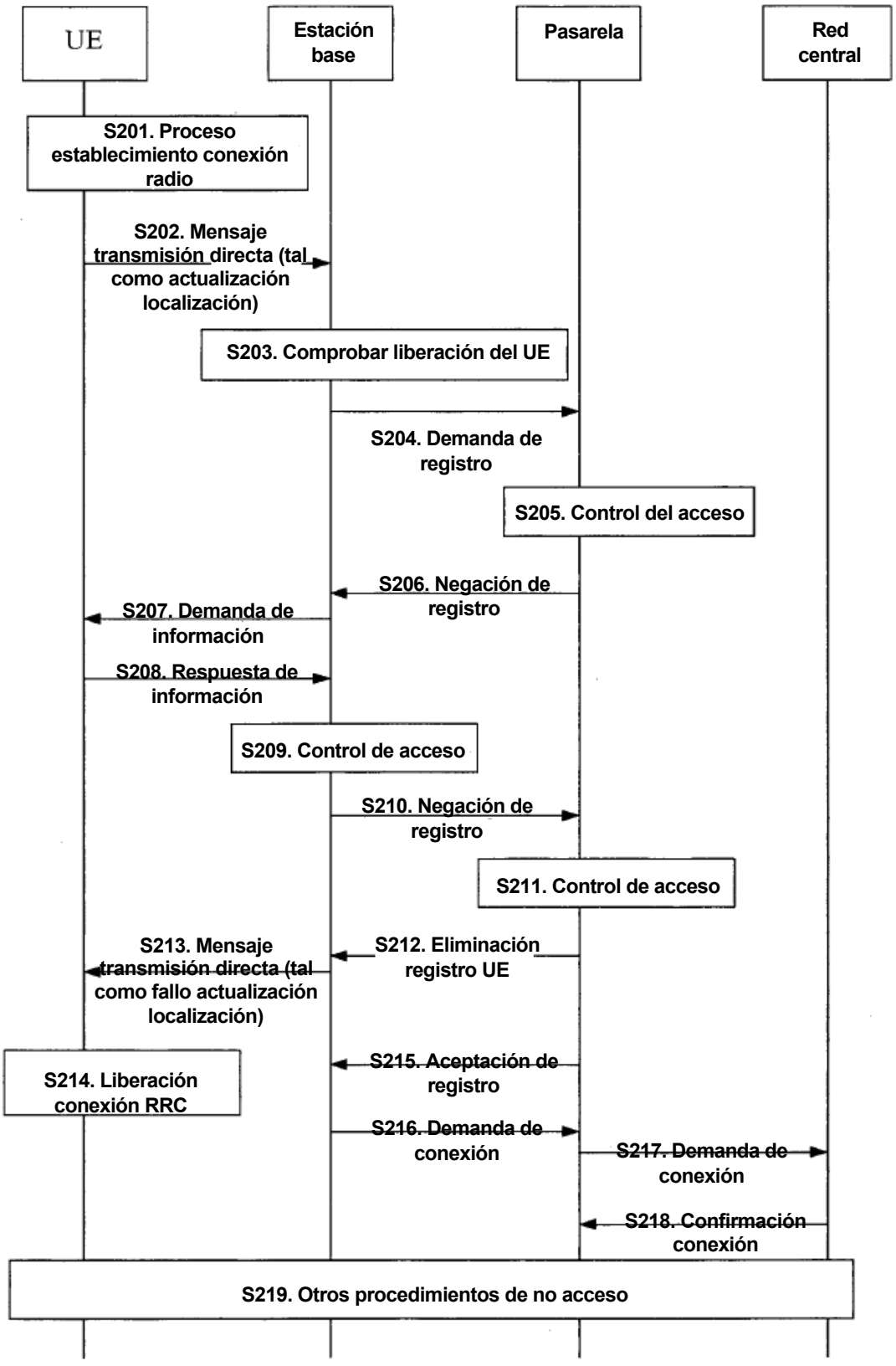
UE
Estación base
Pasarela
Red central
S201. Proceso establecimiento conexión radio
S202. Mensaje transmisión directa (tal como actualización localización)
S203. Comprobar liberación del UE
S204. Demanda de registro
S205. Control del acceso
S206. Negación de registro
S207. Demanda de información
S208. Respuesta de información
S209. Control de acceso
S210. Negación de registro
S211. Control de acceso
S212. Eliminación registro UE
S213. Mensaje transmisión directa (tal como fallo actualización localización)
S214. Liberación conexión RRC
S215. Aceptación de registro
S216. Demanda de conexión
S217. Demanda de conexión
S218. Confirmación conexión
S219. Otros procedimientos de no acceso

FIG. 2

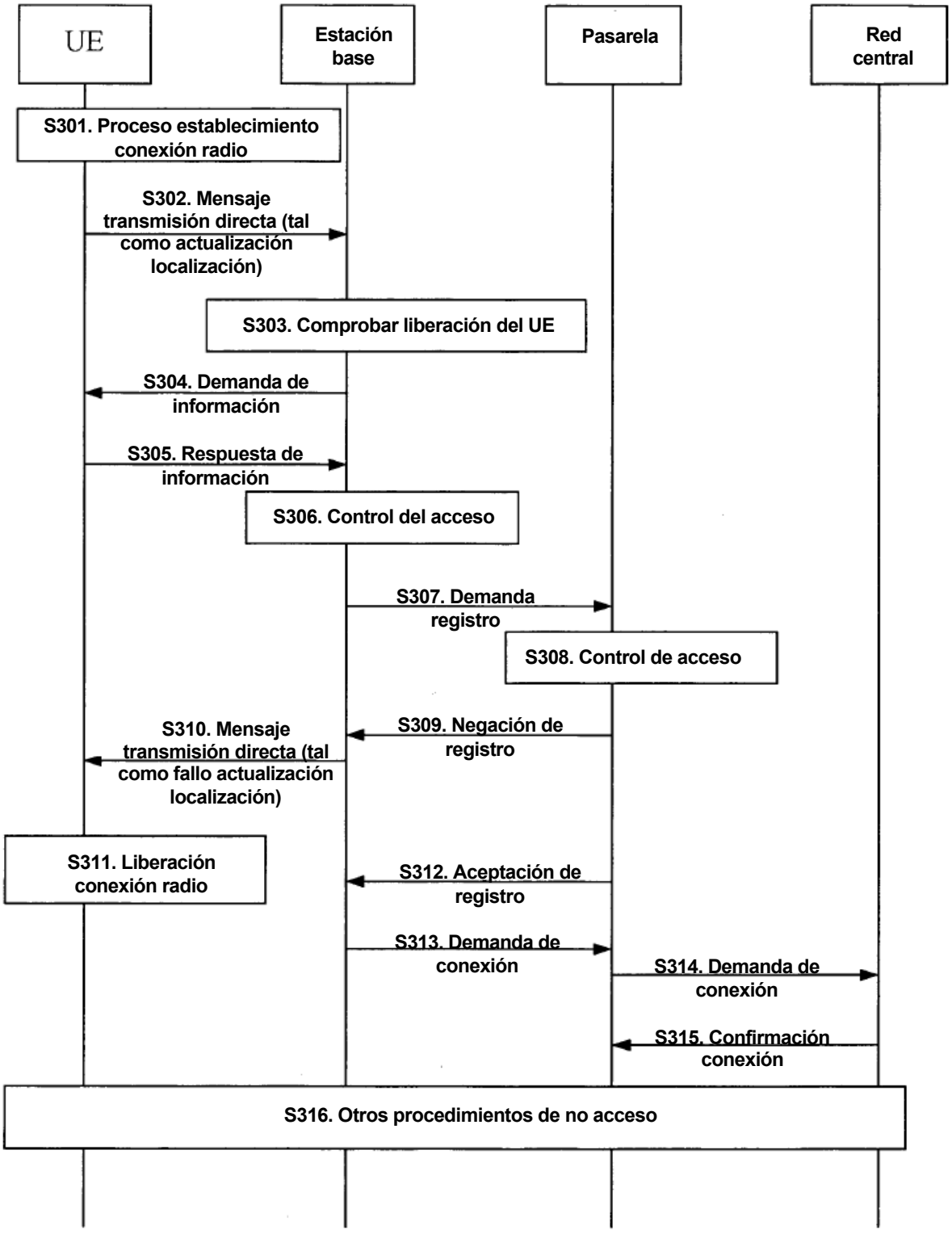
UE
Estación base
Pasarela
Red central
S301. Proceso establecimiento conexión radio
S302. Mensaje transmisión directa (tal como actualización localización)
S303. Comprobar liberación del UE
S304. Demanda de información
S305. Respuesta de información
S306. Control del acceso
S307. Demanda registro
S308. Control de acceso
S309. Negación de registro
S310. Mensaje transmisión directa (tal como fallo actualización localización)
S311. Liberación conexión radio
S312. Aceptación de registro
S313. Demanda de conexión
S314. Demanda de conexión
S315. Confirmación conexión
S316. Otros procedimientos de no acceso

FIG. 3

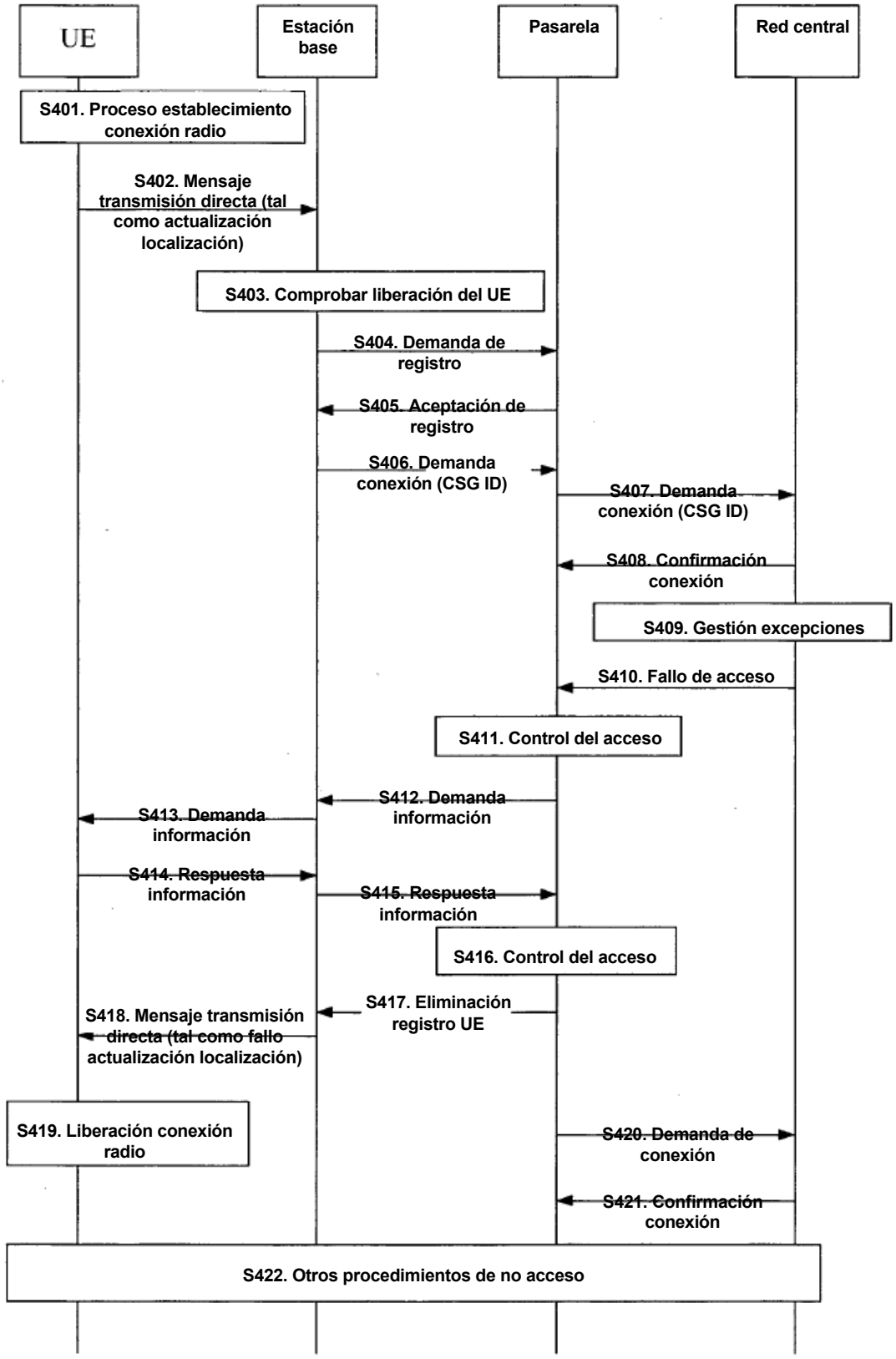
UE
Estación base
Pasarela
Red central
S401. Proceso establecimiento conexión radio
S402. Mensaje transmisión directa (tal como actualización localización)
S403. Comprobar liberación del UE
S404. Demanda de registro
S405. Aceptación de registro
S406. Demanda conexión (CSG ID)
S407. Demanda conexión (CSG ID)
S408. Confirmación conexión
S409. Gestión excepciones
S410. Fallo de acceso
S411. Control del acceso
S412. Demanda información
S413. Demanda información
S414. Respuesta información
S415. Respuesta información
S416. Control del acceso
S417. Eliminación registro UE
S418. Mensaje transmisión directa (tal como fallo actualización localización)
S419. Liberación conexión radio
S420. Demanda de conexión
S421. Confirmación conexión
S422. Otros procedimientos de no acceso

FIG. 4

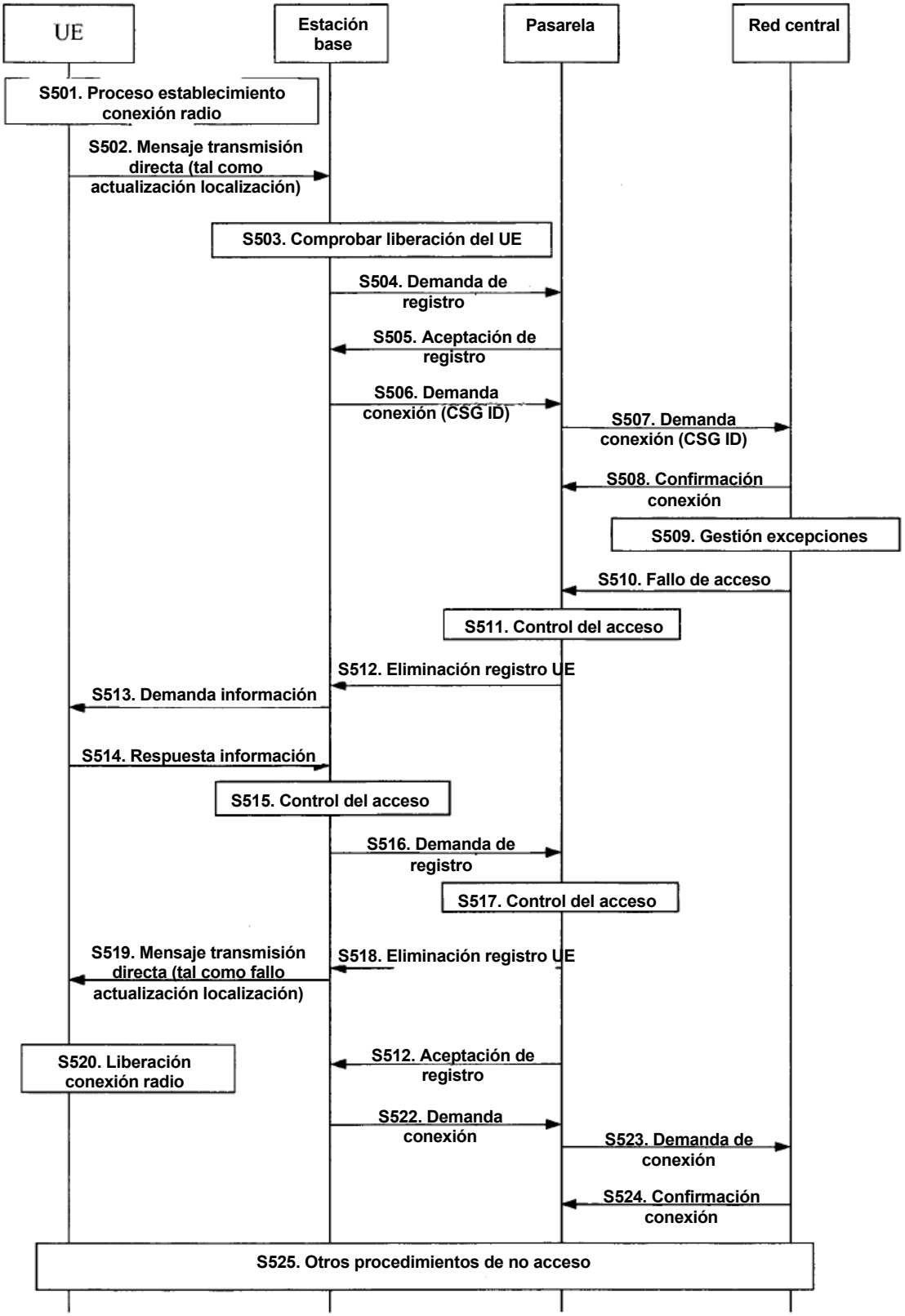
UE
Estación base
Pasarela
Red central
S501. Proceso establecimiento conexión radio
S502. Mensaje transmisión directa (tal como actualización localización)
S503. Comprobar liberación del UE
S504. Demanda de registro
S505. Aceptación de registro
S506. Demanda conexión (CSG ID)
S507. Demanda conexión (CSG ID)
S508. Confirmación conexión
S509. Gestión excepciones
S510. Fallo de acceso
S511. Control del acceso
S512. Eliminación registro UE
S513. Demanda información
S514. Respuesta información
S515. Control del acceso
S516. Demanda de registro
S517. Control del acceso
S519. Mensaje transmisión directa (tal como fallo actualización localización)
S518. Eliminación registro UE
S520. Liberación conexión radio
S512. Aceptación de registro
S522. Demanda conexión
S523. Demanda de conexión
S524. Confirmación conexión
S525. Otros procedimientos de no acceso

FIG. 5

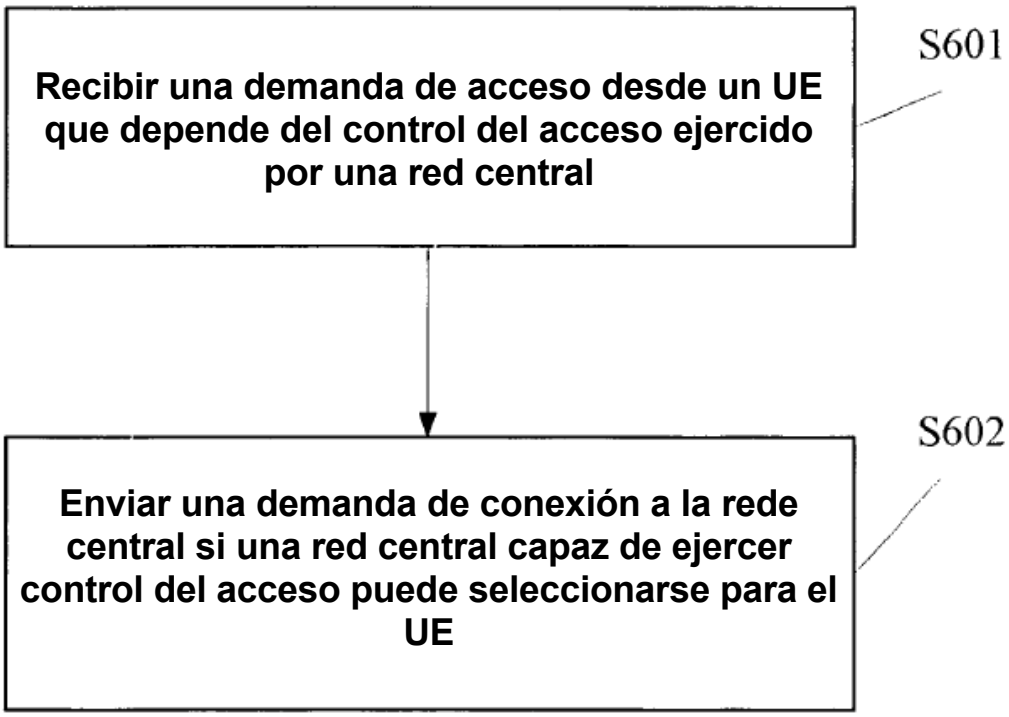
Recibir una demanda de acceso desde un UE que depende del control del acceso ejercido por una red central
S601
Enviar una demanda de conexión a la rede central si una red central capaz de ejercer control del acceso puede seleccionarse para el UE
S602

FIG. 6

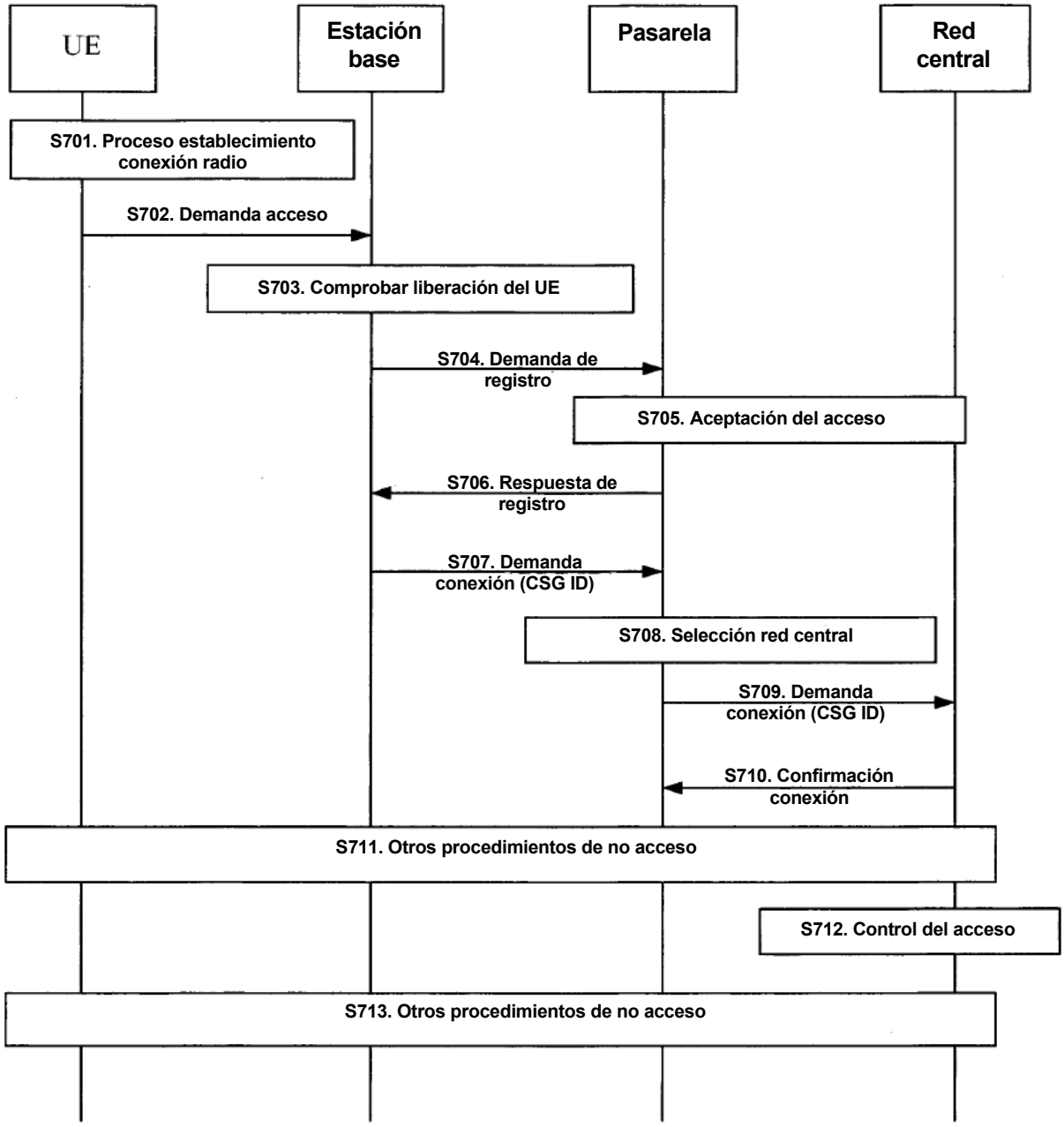
UE
Estación base
Pasarela
Red central
S701. Proceso establecimiento conexión radio
S702. Demanda acceso
S703. Comprobar liberación del UE
S704. Demanda de registro
S705. Aceptación del acceso
S706. Respuesta de registro
S707. Demanda conexión (CSG ID)
S708. Selección red central
S709. Demanda conexión (CSG ID)
S710. Confirmación conexión
S711. Otros procedimientos de no acceso
S712. Control del acceso
S713. Otros procedimientos de no acceso

FIG. 7

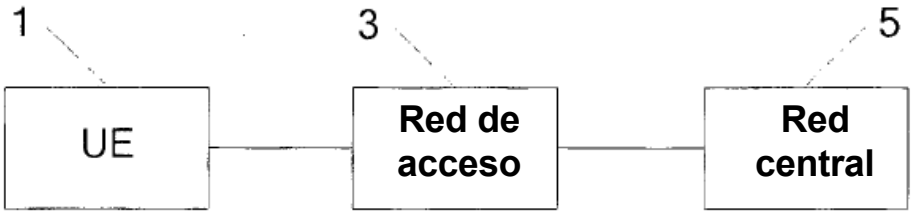
1
3
5
UE
Red de acceso
Red central

FIG. 8

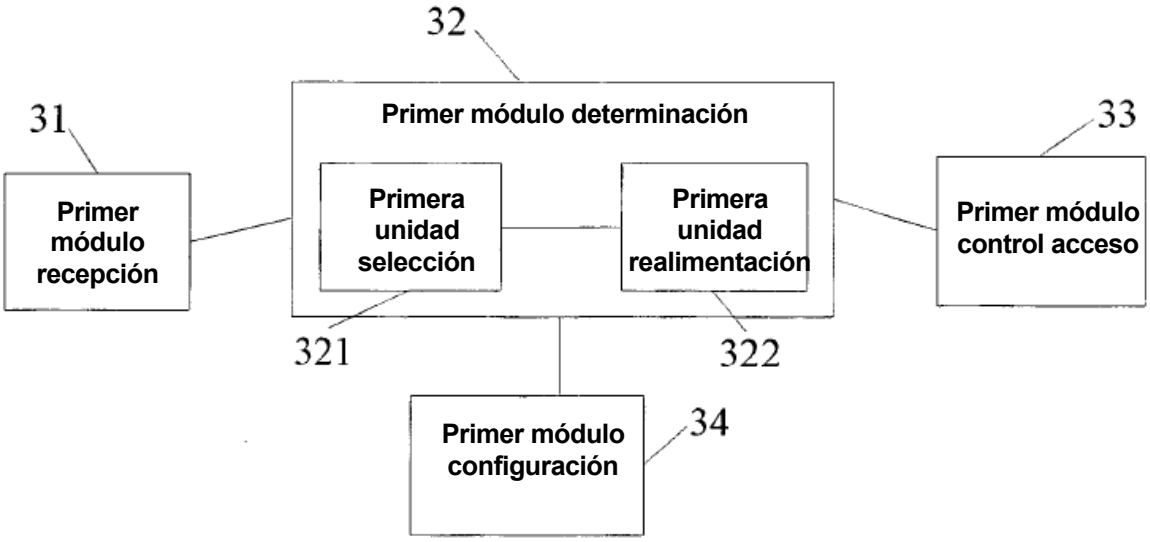
32
Primer módulo determinación
31
33
Primer módulo recepción
Primera unidad selección
Primera unidad realimentación
Primer módulo control acceso
321
322
Primer módulo configuración
34

FIG. 9

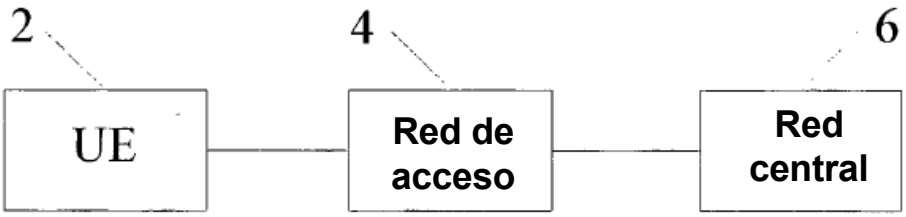
2
4
6
UE
Red de acceso
Red central

FIG. 10

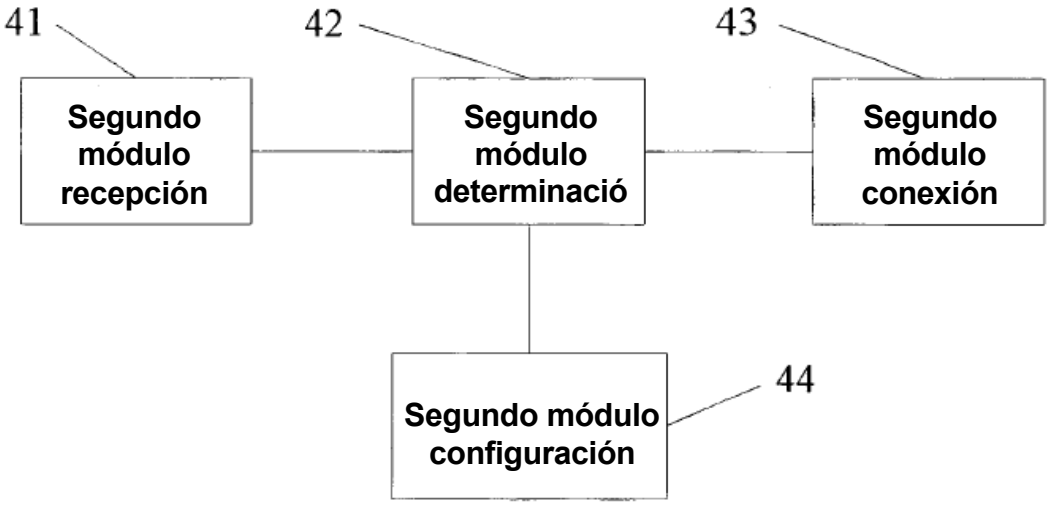
41
42
43
Segundo módulo recepción
Segundo módulo determinació
Segundo módulo conexión
44
Segundo módulo configuración

FIG. 11