

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 442 794**

51 Int. Cl.:

H04W 12/08

(2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **16.08.2010** **E 10742829 (4)**

97 Fecha y número de publicación de la concesión europea: **18.12.2013** **EP 2468025**

54 Título: **Procedimiento y dispositivo para gestionar una célula radioeléctrica privada**

30 Prioridad:

17.08.2009 DE 102009037761

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

13.02.2014

73 Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE

72 Inventor/es:

SCHRÖDER, SÖNKE

74 Agente/Representante:

ARPE FERNÁNDEZ, Manuel

ES 2 442 794 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y dispositivo para gestionar una célula radioeléctrica privada

La invención se refiere a un procedimiento y un dispositivo para la gestión remota de una célula radioeléctrica privada que está conectada a una red radioeléctrica pública. La invención se refiere además a un ordenador de acceso para una célula radioeléctrica privada y un equipo terminal.

Una célula radioeléctrica privada comprende una estación emisora y receptora que se emplea en zonas privadas relativamente pequeñas, como por ejemplo un edificio, y que amplía una red radioeléctrica de un operador público de radiotelefonía móvil. La utilización de la célula radioeléctrica privada es posible con equipos conformes con el estándar de comunicación correspondiente. La utilidad de una célula radioeléctrica privada consiste, entre otras cosas, en la puesta en explotación de lugares difíciles de alcanzar desde el punto de vista de la técnica de radiocomunicación y también en la ampliación de la capacidad en zonas ya abastecidas. El enlace de la célula radioeléctrica privada a la red radioeléctrica pública del operador de radiotelefonía móvil se realiza habitualmente mediante conexiones privadas ya existentes, con lo que el proveedor de la red radioeléctrica pública se ahorra el coste de líneas arrendadas.

La gestión de una célula radioeléctrica privada de este tipo se realiza normalmente a través de un administrador, que está conectado a una unidad de mando (por ejemplo un ordenador de pasarela (*gateway*)) de la célula radioeléctrica privada. Para gestionar la célula radioeléctrica privada es necesaria la presencia del administrador en el ordenador, por ejemplo para permitir la utilización de la célula radioeléctrica privada a un equipo terminal desconocido para la misma.

Una célula radioeléctrica privada en una red de comunicación UMTS (Universal Mobile Telecommunications System [Sistema de telecomunicaciones móviles universales]) se conoce como femtocélula, cuya utilización es posible con cualquier teléfono con capacidad 3G (3rd Generation [3ª generación]) o UMTS. Una femtocélula así se integra de forma complementaria en redes de radiotelefonía móvil públicas de manera que se realice una transferencia exenta de interrupciones de las conexiones entre la femtocélula y la red UMTS. En la mayoría de los casos, el enlace a la red UMTS se realiza mediante una conexión de banda ancha a Internet. Aquí, la femtocélula se conecta por cable a una pasarela de Internet privada, por regla general en forma de un módem DSL.

El documento D1 (US2009/119762) describe un sistema de acceso a red con el que puede controlarse el acceso de un cliente WLAN a una WLAN en función de la posición del cliente WLAN. Con este fin, el sistema de acceso a red incluye una unidad de mando central ("central controller [controlador central]") 42 en comunicación con un servidor de localización ("location server") 22, que contiene información sobre la posición de un cliente WLAN y está configurado para tomar la decisión "¿Acceso a WLAN sí/no?". Dependiendo de esta decisión del servidor de localización 22, la unidad de mando central 42 autoriza o no el acceso del cliente WLAN a una WLAN.

Un objetivo de la presente invención es indicar un procedimiento y un dispositivo que permitan una gestión mejorada de una célula radioeléctrica privada. Otro objetivo es indicar un ordenador de acceso, un equipo terminal y un dispositivo que faciliten la administración de una célula radioeléctrica privada.

Estos objetivos se logran mediante el objeto de las reivindicaciones independientes.

La invención crea un procedimiento para la gestión remota de una célula radioeléctrica privada que está conectada a una red radioeléctrica pública. En el procedimiento, un equipo terminal desconocido para la célula radioeléctrica se autentica frente a un ordenador de acceso de la célula radioeléctrica privada. Una vez autenticado el equipo terminal desconocido, el ordenador de acceso transmite a un equipo de comunicación que gestiona la célula radioeléctrica privada, en forma de un equipo terminal de radiocomunicación móvil, un primer mensaje con el que se solicita la utilización de la célula radioeléctrica privada por parte del equipo terminal desconocido o la utilización de una instalación enlazada con la célula radioeléctrica privada. El ordenador de acceso puede ser por ejemplo un dispositivo de encaminamiento (*router*) de la célula radioeléctrica. El equipo de comunicación encargado de la gestión, transmite al ordenador de acceso un segundo mensaje que permite la utilización, si se da conformidad a la utilización solicitada de la célula radioeléctrica privada por parte del equipo terminal desconocido o su usuario. La utilización solicitada de la célula radioeléctrica privada es denegado al equipo terminal desconocido o su usuario si éste no recibe conformidad del equipo de comunicación.

La denegación de la utilización de la célula radioeléctrica privada al equipo terminal desconocido puede realizarse, por ejemplo, transmitiendo la denegación correspondiente en forma de una fecha en el segundo mensaje, que es transmitido por el equipo de comunicación encargado de la gestión al ordenador de acceso o al equipo terminal desconocido.

El procedimiento según la invención permite la utilización o la autorización de una célula radioeléctrica privada también en ausencia del propietario o administrador, ya que para la gestión de una autorización de acceso los datos pueden intercambiarse entre equipos terminales de radiotelefonía móvil convencionales.

Según una configuración conveniente, el equipo terminal desconocido, por ejemplo un primer equipo terminal de radiocomunicación móvil, comprende una primera aplicación que gestiona el proceso de autenticación frente al ordenador de acceso de la célula radioeléctrica privada. Al mismo tiempo, es especialmente conveniente que la aplicación esté almacenada en un soporte de datos portátil seguro del equipo terminal desconocido. Como soporte de datos portátil puede utilizarse, por ejemplo, una tarjeta SIM (SIM = Subscriber Identity Module [módulo de identidad de abonado]). También es concebible la utilización de una tarjeta chip segura.

Según otra configuración, el equipo de comunicación encargado de la gestión, por ejemplo el equipo terminal de radiocomunicación móvil del administrador de la célula radioeléctrica privada, comprende una segunda aplicación que gestiona un permiso de acceso a la célula radioeléctrica privada y/o equipos terminales autorizados para la utilización de la célula radioeléctrica. El permiso de acceso a la célula radioeléctrica privada puede ser realizado aquí de manera automatizada por el equipo de comunicación encargado de la gestión o manualmente por el usuario del equipo de comunicación que gestiona la red radioeléctrica privada.

Está previsto además que, para la autenticación del equipo terminal desconocido o su usuario por parte del ordenador de acceso, se transmitan datos del equipo terminal desconocido y/o datos personales del usuario del equipo terminal desconocido al ordenador de acceso y éste procese dichos datos. Así pues, todo el proceso de autenticación se efectúa entre el equipo terminal desconocido y el ordenador de acceso de la red radioeléctrica privada. Al equipo de comunicación encargado de la gestión se le transmite la petición del permiso de utilización si la autenticación se ha efectuado con éxito. Por lo tanto, el equipo de comunicación encargado de la gestión o su usuario sólo debe decidir ya si se permite o no al equipo terminal desconocido la utilización de la red radioeléctrica privada.

Según otra configuración conveniente, los equipos terminales autenticados frente al ordenador de acceso se almacenan en una lista del ordenador de acceso. De este modo, la administración de los equipos terminales autorizados resulta fácil de realizar.

Otra configuración prevé la realización de una consulta de código durante el proceso de autenticación por parte del equipo terminal aún desconocido para el ordenador de acceso. La autenticación concluye con un resultado positivo sólo después de que el usuario del equipo terminal aún desconocido haya introducido correctamente el código, con lo que se permite al equipo terminal o su usuario la utilización de la célula radioeléctrica privada y/o el acceso a la instalación. En este último caso es posible por ejemplo impedir así el acceso a instalaciones con un equipo terminal robado. Para aumentar aun más la seguridad es al mismo tiempo conveniente que los datos del equipo terminal necesarios para la autenticación se almacenen en un soporte de datos portátil protegido.

El ordenador de acceso se hace funcionar convenientemente como una parte integrante de la instalación enlazada con la célula radioeléctrica privada. Tal instalación puede tratarse en particular de un sistema de control de acceso, que autorice el acceso a una zona protegida sólo si el equipo terminal desconocido se halla dentro de un área cubierta por la célula radioeléctrica privada o ha sido reconocido por ésta como autorizado para el acceso. De este modo se aumenta la seguridad y se simplifica el control de acceso para edificios y habitáculos mediante la integración del ordenador de acceso en la instalación enlazada con la célula radioeléctrica privada.

También resulta conveniente que, si con un equipo terminal ya autenticado se utiliza o accede repetidamente a la instalación enlazada con la célula radioeléctrica privada, el ordenador de acceso transmita para cada utilización o para cada acceso, un segundo mensaje al equipo de comunicación encargado de la gestión para informar al administrador. De este modo pueden protegerse mejor instalaciones especialmente importantes en cuanto a la seguridad. Esto resulta conveniente, por ejemplo, en caso de una ausencia prolongada. En suma se mejora la seguridad de un control de acceso para edificios o habitáculos.

En otra configuración se transmiten adicionalmente al ordenador de acceso datos de imagen en el primer mensaje transmitido por el equipo terminal desconocido al ordenador de acceso de la célula radioeléctrica privada.

Según otra configuración conveniente, la célula radioeléctrica gestionada es una femtocélula, es decir una célula radioeléctrica UMTS privada, cuya utilización es posible con cualquier teléfono con capacidad 3G o UMTS.

Otra configuración conveniente prevé que la célula radioeléctrica privada esté conectada a la red radioeléctrica móvil pública mediante una conexión de comunicación alámbrica y/o inalámbrica. La conexión de comunicación entre la célula radioeléctrica privada y la red radioeléctrica pública puede realizarse por ejemplo mediante una conexión DLS a través de Internet.

La invención crea además un ordenador de acceso para una célula radioeléctrica privada que está conectada a una red radioeléctrica pública. El ordenador de acceso según la invención está configurado para autenticar un equipo terminal desconocido para la célula radioeléctrica y, una vez autenticado el equipo terminal desconocido, transmitir a un equipo de comunicación que gestiona la célula radioeléctrica privada, en forma de un equipo terminal de radiocomunicación móvil, un primer mensaje con el que se solicita la utilización de la célula radioeléctrica privada por parte del equipo terminal desconocido o la utilización de una instalación enlazada con la célula radioeléctrica privada. El ordenador de acceso está configurado además para recibir un segundo mensaje enviado por el equipo

de comunicación encargado de la gestión y, en función de éste, dar conformidad a la utilización solicitada de la célula radioeléctrica privada por parte del equipo terminal desconocido o su usuario o denegar dicha utilización.

Un equipo terminal según la invención se distingue porque está configurado para autenticarse frente a un ordenador de acceso de una célula radioeléctrica privada que está conectada a una red radioeléctrica pública.

- 5 Un dispositivo según la invención para la gestión remota de una célula radioeléctrica privada que está conectada a una red radioeléctrica pública comprende un ordenador de acceso según la invención, así como un equipo de comunicación para gestionar la célula radioeléctrica privada, en forma de un equipo terminal de radiocomunicación móvil, y un equipo terminal del tipo anteriormente descrito.

A continuación se describe la invención más detalladamente por medio de un ejemplo de realización.

- 10 La única figura muestra, en una representación esquemática, un dispositivo según la invención para la gestión remota de una célula radioeléctrica privada HNB que está conectada a una red radioeléctrica pública MCN mediante una conexión de comunicación KV. La red radioeléctrica pública MCN se trata, por ejemplo, de una red radioeléctrica móvil UMTS (UMTS - Universal Mobile Telecommunication System [sistema de telecomunicaciones móviles universales]). En este caso, la célula radioeléctrica privada se denomina femtocélula, que está configurada, por
15 ejemplo, según el estándar 3GPP TS 33.820 y en éste se denomina "Home(e)NodeB [nodoB propio(e)]" o H(e)NB. La femtocélula permite la utilización de un teléfono con capacidad 3G o UMTS en el área cubierta por la célula radioeléctrica (por ejemplo en un edificio), con lo que se amplía la red radioeléctrica pública MCN de un operador de radiotelefonía móvil. La femtocélula HNB está conectada a Internet IN, por ejemplo, mediante una línea DSL L1. Internet IN está conectada a la red radioeléctrica pública MCN mediante otra conexión de comunicación L2, que
20 puede ser de naturaleza alámbrica o inalámbrica.

- La femtocélula es gestionada por un administrador, que se halla en posesión de un equipo de comunicación encargado de la gestión AEG, en forma de un equipo terminal de radiocomunicación móvil. El equipo de comunicación encargado de la gestión AEG es, por ejemplo, un equipo de comunicación con capacidad 3G o UMTS, que puede comunicarse de forma inalámbrica con un ordenador de acceso ROU, por ejemplo un dispositivo de encaminamiento (*router*) de femtocélula, de la célula radioeléctrica privada HNB.
25

- Con el procedimiento descrito a continuación se permite al usuario del equipo de comunicación encargado de la gestión AEG permitir, mediante una gestión remota, la utilización de la célula radioeléctrica privada HNB por parte de un equipo terminal desconocido EG, por ejemplo un equipo de comunicación con capacidad 3G o UMTS. En el equipo terminal desconocido EG al que ha de permitirse la utilización de la femtocélula HNB, se encuentra
30 almacenada con este fin una aplicación que permite una comunicación con el ordenador de acceso ROU en lo que se refiere a un permiso de utilización. La aplicación está almacenada preferentemente en una tarjeta SIM protegida (SIM = Subscriber Identity Module [módulo de identidad de abonado]) del equipo terminal desconocido EG. Si el usuario del equipo terminal EG desconocido para la femtocélula desea autenticarse frente al ordenador de acceso ROU, se transmite una petición correspondiente del equipo terminal desconocido EG al ordenador de acceso ROU.

- 35 El ordenador de acceso ROU recibe la petición, preferentemente incluyendo datos personales del usuario, y registra los datos de autenticación del equipo terminal desconocido EG. El ordenador de acceso ROU reenvía la petición, por ejemplo en forma de un mensaje SMS, directamente, es decir dentro de la femtocélula, o a través de la conexión de comunicación KV y la red radioeléctrica pública, al equipo de comunicación AEG. Si el administrador desea permitir al equipo terminal desconocido EG la utilización de la femtocélula, puede hacerlo por medio de un mensaje de confirmación, por ejemplo un mensaje SMS, transmitido al ordenador de acceso ROU y/o al equipo terminal desconocido EG. La utilización puede permitirse una única vez o también de un modo general. Si el administrador no desea permitir la utilización de la femtocélula por parte del equipo terminal EG, se deniega la utilización, lo que
40 puede realizarse por medio de un mensaje correspondiente del equipo de comunicación AEG al ordenador de acceso ROU y/o al equipo terminal desconocido EG.

- 45 En el equipo de comunicación AEG del administrador de la femtocélula HNB está preferentemente almacenada una aplicación que permita gestionar el ordenador de acceso ROU o la interfaz de radiocomunicación entre equipos terminales autorizados y la femtocélula HNB. De este modo se ofrece al administrador del equipo de comunicación AEG la posibilidad de gestionar mediante su equipo de comunicación AEG todas las funciones, incluyendo la lista de los usuarios autorizados para la femtocélula HNB.

- 50 Este procedimiento permite en particular gestionar la femtocélula HNB también en ausencia del propietario o administrador de la misma y permitir o denegar a usuarios o equipos terminales desconocidos la utilización de la femtocélula.

- El procedimiento según la invención puede utilizarse también para gestionar una instalación enlazada con la célula radioeléctrica privada, por ejemplo un sistema de control de acceso a un edificio o habitáculo. La instalación puede
55 tratarse también de una instalación de alarma. El ordenador de acceso es en este caso una parte integrante de la instalación enlazada con la célula radioeléctrica, que pide un permiso de acceso a través de una consulta remota al propietario de la célula radioeléctrica o a su equipo de comunicación encargado de la gestión.

El usuario del equipo terminal desconocido EG que solicita un permiso de utilización pide, por ejemplo un permiso de acceso a un edificio o habitáculo. Esto puede realizarse por ejemplo ejecutando la aplicación correspondiente, almacenada en el equipo terminal desconocido EG, que transmite un mensaje de petición al ordenador de acceso ROU. Como alternativa, el usuario puede pulsar un botón de timbre en el edificio o habitáculo, con lo que se genera el mensaje de petición y se transmite el mismo al ordenador de acceso ROU. El ordenador de acceso ROU recibe la petición, incluyendo los datos personales del usuario o de su equipo terminal desconocido EG. En particular, el ordenador de acceso ROU registra los datos de autenticación del equipo terminal desconocido EG, almacenados por ejemplo en su soporte de datos portátil seguro (tarjeta SIM), y reenvía la petición, directamente o a través de la conexión de comunicación KV, al equipo de comunicación encargado de la gestión AEG del administrador de la instalación, siempre que en el ordenador de acceso ROU aún no esté almacenado ningún permiso de utilización al usuario o su equipo terminal desconocido EG. En caso de una confirmación positiva por parte del administrador a través de su equipo de comunicación AEG, se autoriza el acceso al usuario del equipo terminal desconocido EG. En caso de una confirmación negativa, se deniega el acceso a la instalación.

Para aumentar la seguridad es posible, por ejemplo utilizando un MMS (Multimedia Service [servicio multimedia]), enviar conjuntamente con fines de control una fotografía o un vídeo actual de la zona de entrada. Este procedimiento permite el control de acceso para personas que no o aún no están depositadas en una memoria del ordenador de acceso ROU.

El ordenador de acceso puede emplearse también como parte integrante de una instalación de alarma para un edificio o habitáculo, autorizándose el acceso, sólo si un determinado equipo terminal se halla dentro del alcance de radio de la célula radioeléctrica privada y está autenticado. De este modo puede aumentarse la seguridad para instalaciones de alarma. Además, se simplifica el control de acceso para edificios y habitáculos. El acceso a un edificio o habitáculo es posible sólo si el ordenador de acceso ha registrado un equipo terminal correspondientemente autorizado para el acceso. Los equipos terminales autorizados pueden por ejemplo almacenarse o administrarse en una lista en el TrE (Trusted Environment [entorno de confianza]) o en el HPM (Hosting Party Module [módulo de participante de anfitrión]) del ordenador de acceso ROU.

La unidad de control de acceso propiamente dicha, como por ejemplo una cerradura eléctrica de puerta, o una instalación de alarma, está conectada al ordenador de acceso ROU mediante una conexión de comunicación. La conexión de comunicación puede realizarse opcionalmente mediante un cable USB, una conexión LAN, una conexión WLAN o una conexión WUSB. Como se desprende de la descripción precedente, el ordenador de acceso ROU se utiliza únicamente para la autenticación, mientras que el control de acceso propiamente dicho se realiza mediante la unidad de control de acceso.

Para aumentar la seguridad puede realizarse adicionalmente una consulta del PIN (número de identificación personal) en el equipo terminal. El acceso no se autoriza hasta haberse introducido correctamente el PIN. Esto impide, por ejemplo el acceso a edificios/habitáculos con un equipo terminal EG robado. Por motivos de seguridad, los datos del equipo terminal EG necesarios para la autenticación se almacenan convenientemente en la tarjeta SIM protegida. La autenticación se realiza convenientemente de acuerdo con las especificaciones habituales en 3GPP, tales como las publicadas por ejemplo en la especificación TS 33.820.

En zonas especialmente importantes para la seguridad es posible, por ejemplo, transmitir en cada acceso a la zona protegida un mensaje al administrador de la célula radioeléctrica privada mediante el ordenador de acceso. Esto puede resultar conveniente por ejemplo en caso de una ausencia prolongada, como por ejemplo unas vacaciones. Este mensaje transmitido regularmente puede estar configurado como un mensaje SMS y bien transmitirse directamente del ordenador de acceso ROU al equipo de comunicación encargado de la gestión AEG o bien transmitirse mediante la conexión de comunicación KV y la red radioeléctrica pública a éste.

REIVINDICACIONES

1. Procedimiento para la gestión remota de una célula radioeléctrica privada (HNB) que está conectada a una red radioeléctrica pública (MCN), en el que
 - un equipo terminal (EG) desconocido para la célula radioeléctrica se autentica frente un ordenador de acceso (ROU) de la célula radioeléctrica privada (HNB),
 - el ordenador de acceso (ROU), una vez autenticado el equipo terminal desconocido (EG), transmite a un equipo de comunicación móvil (AEG) que gestiona la célula radioeléctrica privada (HNB), un primer mensaje con el que se solicita la utilización de la célula radioeléctrica privada (HNB) por parte del equipo terminal desconocido (EG) o la utilización de una instalación enlazada con la célula radioeléctrica privada (HNB),
- estando el ordenador de acceso (ROU) configurado para transmitir dicho primer mensaje al equipo de comunicación móvil encargado de la gestión (AEG) dentro de la célula radioeléctrica privada (HNB) o a través de la red radioeléctrica pública (MCN),
 - el equipo de comunicación móvil encargado de la gestión (AEG) transmite al ordenador de acceso (ROU) o al equipo terminal desconocido (EG), un segundo mensaje que permite la utilización, si se da conformidad a la utilización solicitada de la célula radioeléctrica privada (HNB) por parte del equipo terminal desconocido (EG) o su usuario, y
 - la utilización solicitada de la célula radioeléctrica privada (HNB) por parte del equipo terminal desconocido (EG) o su usuario se deniega si no se recibe conformidad del equipo de comunicación móvil (AEG), tratándose el equipo de comunicación móvil (AEG) de un equipo terminal de radiocomunicación móvil.
2. Procedimiento según la reivindicación 1, en el que el equipo terminal desconocido (EG) comprende una primera aplicación, que gestiona el proceso de autenticación frente al ordenador de acceso (ROU) de la célula radioeléctrica privada (HNB).
3. Procedimiento según la reivindicación 2, en el que la aplicación está almacenada en un soporte de datos portátil seguro del equipo terminal desconocido.
4. Procedimiento según una de las reivindicaciones precedentes, en el que el equipo de comunicación encargado de la gestión (AEG) comprende una segunda aplicación que gestiona un permiso de acceso a la célula radioeléctrica privada (HNB) y/o equipos terminales (EG) autorizados a la utilización de la célula radioeléctrica.
5. Procedimiento según una de las reivindicaciones precedentes, en el que, para la autenticación del equipo terminal desconocido (EG) o su usuario por parte del ordenador de acceso (ROU), se transmiten datos del equipo terminal desconocido (EG) y/o datos personales del usuario del equipo terminal desconocido (EG) al ordenador de acceso (ROU) y éste procesa dichos datos.
6. Procedimiento según una de las reivindicaciones precedentes, en el que los equipos terminales (EG) autenticados frente al ordenador de acceso (ROU) se almacenan en una lista de dicho ordenador de acceso (ROU).
7. Procedimiento según una de las reivindicaciones precedentes, en el que durante el proceso de autenticación por parte del equipo terminal (EG) aún desconocido para el ordenador de acceso (ROU) se realiza una consulta de código.
8. Procedimiento según una de las reivindicaciones precedentes, en el que el ordenador de acceso (ROU) se hace funcionar como una parte integrante de la instalación enlazada con la célula radioeléctrica privada (HNB).
9. Procedimiento según la reivindicación 8, en el que la instalación es un sistema de control de acceso que está enlazado a la célula radioeléctrica privada (HNB).
10. Procedimiento según la reivindicación 8 o 9, en el que, si con un equipo terminal (EG) ya autenticado se usa o se accede repetidamente a la instalación enlazada con la célula radioeléctrica privada, el ordenador de acceso (ROU) transmite para cada utilización o para cada acceso, un segundo mensaje al equipo de comunicación encargado de la gestión (AEG) para informar al administrador.
11. Procedimiento según una de las reivindicaciones 8 a 10, en el que en el primer mensaje se transmiten adicionalmente al ordenador de acceso (ROU) datos de imagen.
12. Procedimiento según una de las reivindicaciones precedentes, en el que la célula radioeléctrica gestionada es una femtocélula.

13. Procedimiento según una de las reivindicaciones precedentes, en el que la célula radioeléctrica privada (HNB) está conectada a la red radioeléctrica móvil pública (MCN) mediante una conexión de comunicación (KV) alámbrica y/o inalámbrica.

5 14. Ordenador de acceso para una célula radioeléctrica privada (HNB) que está conectada a una red radioeléctrica pública (MCN), que está configurado para

- autenticar un equipo terminal (EG) desconocido para la célula radioeléctrica,

10 - una vez autenticado, el equipo terminal desconocido (EG), transmitir a un equipo de comunicación móvil (AEG) que gestiona la célula radioeléctrica privada (HNB) un primer mensaje con el que se solicita la utilización de la célula radioeléctrica privada (HNB) por parte del equipo terminal desconocido (EG) o la utilización de una instalación enlazada con la célula radioeléctrica privada (HNB),

estando el ordenador de acceso configurado para transmitir el primer mensaje al equipo de comunicación móvil encargado de la gestión (AEG) dentro de la célula radioeléctrica privada (HNB) o a través de la red radioeléctrica pública (MCN),

15 - recibir un segundo mensaje enviado por el equipo de comunicación móvil encargado de la gestión (AEG) y, en función de éste, dar conformidad para la utilización solicitado de la célula radioeléctrica privada (HNB) por parte del equipo terminal desconocido (EG) o su usuario o denegar la utilización, tratándose el equipo de comunicación móvil (AEG) de un equipo terminal de radiocomunicación móvil.

15. Sistema para la gestión remota de una célula radioeléctrica privada (HNB) que está conectada a una red radioeléctrica pública (MCN), que comprende

20 - un ordenador de acceso según la reivindicación 14 y

- un equipo de comunicación móvil (AEG) para gestionar la célula radioeléctrica privada (HNB), tratándose el equipo de comunicación móvil (AEG) de un equipo terminal de radiocomunicación móvil.

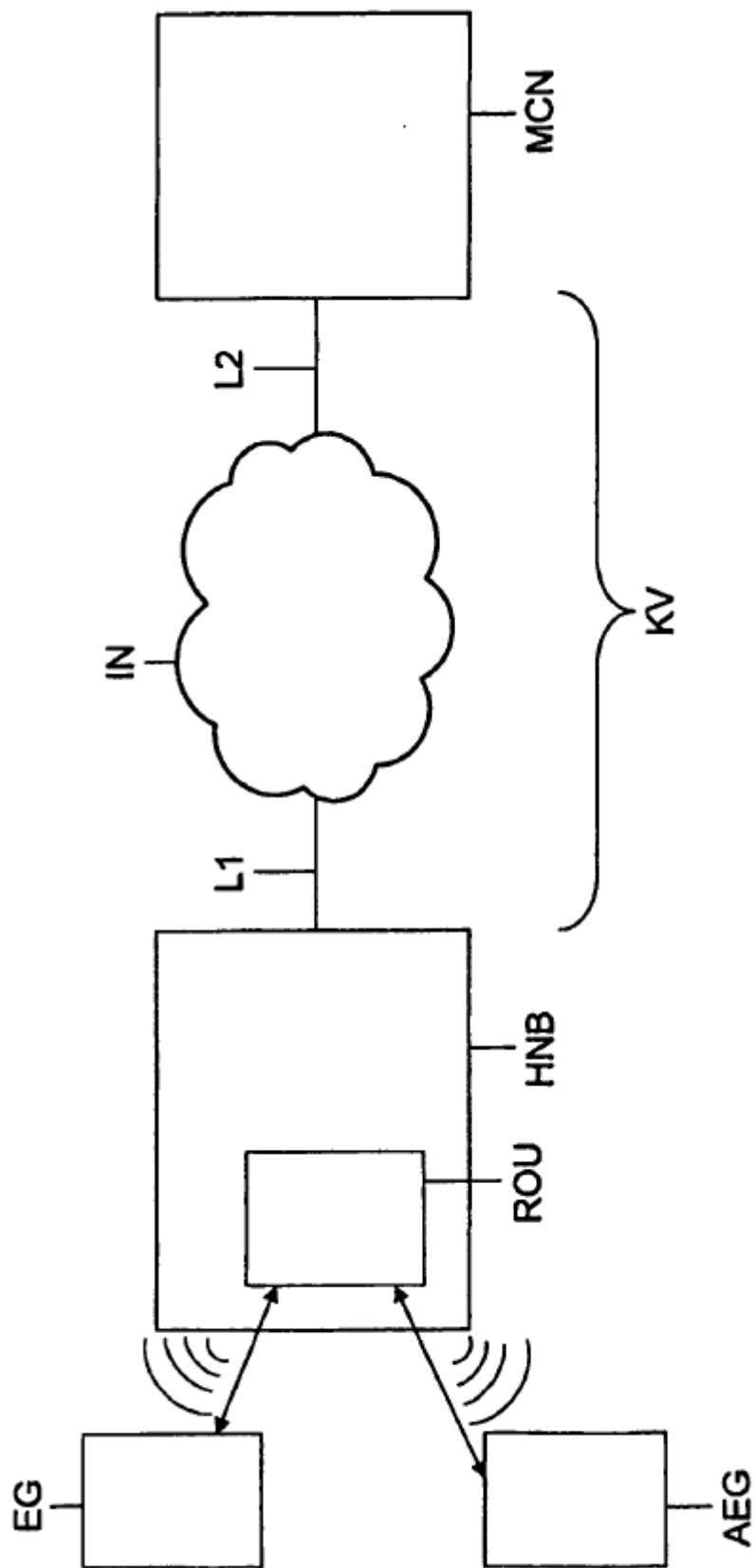


Fig. 1

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- US 2009119762 A [0005]