(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 748 912**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.10.2010 PCT/EP2010/065828**

(87) Fecha y número de publicación internacional: **28.04.2011 WO11048161**

(96) Fecha de presentación y número de la solicitud europea: **20.10.2010 E 10766295 (9)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2019 EP 2491735**

(54) Título: **Dispositivo y procedimiento de gestión de los derechos de acceso a una red sin hilos**

(30) Prioridad:

23.10.2009 FR 0957463

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2020

(73) Titular/es:

IDEMIA IDENTITY & SECURITY FRANCE (100.0%)
2, Place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

PEPIN, CYRILLE y
LECOCQ, FRANÇOIS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Dispositivo y procedimiento de gestión de los derechos de acceso a una red sin hilos

El presente invento se refiere a un dispositivo y a un procedimiento de gestión de los derechos de acceso a una red sin hilos.

Hoy en día, las redes de comunicación y de una manera más particular la red Internet toman una importancia cada vez más grande en la comunicación ya sea en el plano personal o en el plano profesional. Los usuarios sienten el deseo de poder conectarse a esta red de una manera permanente, si es posible, o que tienda a ser permanente. En este contexto, uno de los medios de acceso privilegiados es el acceso sin hilos que pueda hacerse desde un terminal móvil de comunicación. En particular, el acceso según la norma Wi-Fi normalizada por IEEE (Institute of Electrical and Electronics Engineers, en inglés) en la familia de la norma 802.11, tiende a generalizarse. Este acceso se realiza mediante el despliegue de los puntos de acceso Wi-Fi conectados a la red de información y que permite a las terminales, típicamente un ordenador portátil, establecer una conexión con este punto de acceso. Una vez establecida esta conexión, el tráfico de datos se turna con el punto de acceso entre el terminal y la red de comunicación.

Tales puntos de acceso son desplegados por múltiples actores económicos. Se pueden citar los accesos públicos generados por colectividades en establecimientos públicos como las bibliotecas. Se puede citar también el acceso puesto a disposición de los viajeros en los aeropuertos, las estaciones y los hoteles. Las empresas tienden igualmente a desplegar punto de acceso en su red informática y en Internet, por una parte, para sus asalariados, y por otra parte para los visitantes.

Algunos de estos accesos tienen vocación de ser abiertos de una manera no limitada o no controlada, típicamente un acceso público o en algunos casos un acceso para los asalariados en la empresa. Por el contrario, otros accesos tienen vocación de estar limitados y controlados, ya sea por razones de seguridad con los visitantes en una empresa o por que se desea un acceso con moneda, típicamente en un hotel. Estos límites pueden ser geográficos, el acceso del visitante está limitado, por ejemplo, a una sala de reuniones en una empresa. Estos límites pueden ser temporales, se puede utilizar un sistema de créditos de conexión vendidos en un hotel o en un garaje, por ejemplo.

Hoy en día, estas limitaciones son generadas generalmente por un sistema AAA (Authentication, Authorization and Accounting, en inglés) de autentificación, autorización y de compatibilidad central bajo la forma de cuentas de los usuarios a los cuales están asociadas las limitaciones. Este sistema es muy pesado de generar, cualquier venta de un servicio que necesite una puesta al día del sistema central y la distribución de identificadores de conexión asociados al usuario.

El documento WO2004/034205 A2 describe un sistema de control y de gestión de acceso a las redes, y de una manera más particular a WiFi, basado en la utilización de un token USB que contiene de una manera ventajosa una tarjeta con un chip. El documento WO2007/056383 A1 describe una gestión de derecha de acceso centralizado que genera unas reglas para un conjunto de puntos de acceso. El documento US2007/025334 A1 describe un sistema en el cual un terminal móvil se adjunta a un componente de seguridad para generar unas listas de autorizaciones (ACL) para los puntos de acceso. El documento EP 1 701 478 A1 describe un sistema y un procedimiento para configurar unos interfaces sin hilos, basado en la utilización de un stick USB-WLAN.

El invento trata de resolver los problemas precedentes mediante la utilización de unos dispositivos de conexión sin hilos, de una manera ventajosa basados en una tarjeta con un chip, que permite la conexión sin hilos a la red una vez conectados a un terminal. Estos dispositivos integran unos medios de gestión temporal y/o geográfica de acceso a la red y unos medios de autentificación. Estos dispositivos pueden ser fácilmente programados por la entidad generadora del servicio y distribuidos a continuación a los usuarios.

El invento está definido en las reivindicaciones 1 a 8.

El invento se refiere a un dispositivo de acceso a una red sin hilos que incluye unos medios de conexión a un dispositivo huésped; unos medios de conexión a un punto de acceso a una red sin hilos; unos medios para abrir una conexión con el punto de acceso a la red sin hilos a la recepción de una solicitud de activación de la conexión de una manera que permita el acceso a la red sin hilos en la máquina huésped a la que está conectado y unos medios de gestión de los derechos de acceso a la red sin hilos.

Según un modo particular de realización del invento, al menos los medios de gestión de los derechos de acceso a la red sin hilos están integrados en una tarjeta con un chip.

Según un modo particular de realización del invento, los medios de gestión de los derechos de acceso a la red sin hilos incluyen unos medios de limitar temporalmente este acceso.

Según un modo particular de realización del invento, los medios de gestión de los derechos de acceso a la red sin hilos incluyen un certificado que tiene una duración de validez restringida.

Según un modo particular de realización del invento, los medios de gestión de los derechos de acceso a una red sin hilos, incluyen unos medios para descontar el tiempo de conexión de un crédito programado.

Según un modo particular de realización del invento, los medios de gestión de los derechos de acceso a una red sin hilos, incluyen unos medios para limitar geográficamente este acceso.

Según un modo particular de realización del invento, los medios de gestión de los derechos de acceso a una red sin hilos, incluyen unos medios de gestión de las listas de control del acceso que permitan determinar cuáles conexiones están autorizadas.

El invento se refiere igualmente a un procedimiento de gestión de los derechos de acceso a una red sin hilos que incluye una etapa de recepción de una solicitud de activación de la conexión por parte de un dispositivo de acceso a la red sin hilos que incluye a su vez unos medios de conexión a un dispositivo huésped, unos medios de conexión a un punto de acceso de una red sin hilos y unos medios para abrir una conexión con el punto de acceso de la red sin hilos a la recepción de una solicitud de activación de la conexión de tal manera que permita el acceso a la red sin hilos a la máquina huésped a la que está conectado; una etapa de test de los puntos de acceso disponibles; una etapa de verificación de que al menos un punto de acceso disponible está autorizado; una etapa de conexión si este test es positivo; una etapa negando la conexión si este test es negativo.

El invento se refiere igualmente a un procedimiento de gestión de los derechos de acceso a una red sin hilos que incluye una etapa de recepción de una solicitud de activación de la conexión por parte de un dispositivo de acceso a la red sin hilos que incluye a su vez unos medios de conexión a un dispositivo huésped, unos medios de conexión a un punto de acceso de la red sin hilos y unos medios para abrir una conexión con el punto de acceso de la red sin hilos a la recepción de una solicitud de activación de la conexión de tal manera que permita el acceso a la red sin hilos a la máquina huésped a la que está conectado; una etapa de test del tiempo disponible; una etapa de test de la disponibilidad de la red; una etapa de conexión si estos dos tests son positivos; una etapa negando la conexión si uno de estos test es negativo..

Las características del invento mencionadas anteriormente, así como otras, aparecerán de una manera más clara con la lectura de la siguiente descripción de un ejemplo de realización, estando hecha la citada descripción en relación con los dibujos adjuntos, entre los cuales:

La Figura 1 describe la arquitectura general de un ejemplo del sistema utilizado por el invento.

La Figura 2 describe la arquitectura material de un ejemplo de realización del invento,

La Figura 3 describe un primer ejemplo del procedimiento de conexión según el invento,

La Figura 4 describe un segundo del procedimiento de conexión según el invento,

La arquitectura general de utilización del invento está ilustrada en la figura 1. En esta figura, se ve un terminal personal 1.9, por ejemplo, un ordenador personal, un ordenador portátil, un asistente personal u otro. El usuario de este terminal 1.9 busca acceder a una red de comunicación 1.1, típicamente Internet. Al estar disponible el acceso a esta red en su entorno bajo la forma de uno o varios puntos de acceso sin hilos 1.2 a 1.5, estos puntos de acceso son típicamente bornes de acceso Wi-Fi. Estando estos bornes generalmente conectados entre sí por una red local 1.6, y conectada ella a su vez a una red de comunicación 1.1 por una conexión 1.7. Es corriente hoy en día que los terminales estén dotados a su vez de un interfaz de red Wi-Fi que les permite establecer una conexión con uno de los puntos de acceso para establecer la conexión a la red de comunicación o a una red local a la cual están conectados los bornes de acceso.

El invento se sitúa sin embargo en el marco en el que la autoridad encargada de la gestión de la red local y de los puntos de acceso trata de controlar este acceso. Las razones de esta voluntad pueden ser diversas. Pueden ser razones de seguridad, se quiere controlar quien se conecta y donde, así como los recursos de la red a los cuales el usuario puede tener acceso. En este caso, se puede querer limitar el acceso en ciertos puntos de acceso particular o incluso restringir este acceso a cuentas cuyas autorizaciones serán controladas, por ejemplo, para limitar el acceso a una intranet. Puede ser también la voluntad de utilizar una moneda para el tiempo de conexión. En este caso, es el tiempo de acceso el que se desea poder verificar. Estos diferentes tipos de controles no son nada más que ejemplos, y se pueden utilizar varios o añadir otros sin salirnos del invento.

En este marco, el invento se basa en la difusión por parte de la autoridad de gestión de los accesos de los dispositivos de acceso 1.8 a los usuarios. Estos dispositivos están dotados, por una parte, de un medio de conexión 1.10 al terminal huésped 1.9, típicamente según la norma USB (Universal Serial Bus, en inglés), pero pueden ser utilizados otros tipos de conexiones indiferentemente como la tecnología de conexión Bluetooth, Ethernet u otros. El dispositivo 1.8 está dotado igualmente de unos medios de conexión sin hilos según el protocolo de comunicación utilizado por los puntos de acceso típicamente Wi-Fi. El invento está basado en el hecho de que el dispositivo incluye unos medios de gestión de los derechos de acceso a la red sin hilos. El dispositivo puede verificar entonces que los derechos de acceso son verificados antes de abrir una conexión 1.11 con el punto de acceso y autorizar, por lo tanto, al usuario acceder a la red de comunicación con la ayuda de su terminal. El dispositivo es visto entonces de

una manera ventajosa como un interfaz de la red por parte del terminal. Los puntos de acceso están configurados de una manera ventajosa para prohibir el acceso a cualquier terminal excepto a los dispositivos distribuidos. En algunos modos de realización, los puntos de acceso pueden dar un acceso libre a una lista de terminales conocidos, típicamente los ordenadores utilizados por los colaboradores de una empresa, mientras que los ordenadores desconocidos, los de los visitantes, no pueden conectarse nada más que utilizando un dispositivo según el invento que les es distribuido.

La Figura 2 ilustra la arquitectura material de un ejemplo de realización del dispositivo según el invento. Este modo de realización está basado en la utilización ventajosa de una tarjeta con un chip 2.1. Esta tarjeta con un chip está conectada a un lector de tarjetas con chip del tipo USB 2.10, conectada a su vez al terminal 2.13 en un puerto USB 2.14. La tarjeta con chip puede estar integrada igualmente en el dispositivo que se presenta entonces bajo la forma de una llave USB que contiene un periférico Wi-Fi y una tarjeta con chip integrada. A pesar de que puede ser utilizada en un periférico Wi-Fi conectable por USB, corrientemente llamado “llave USB Wi-Fi” simplemente añadiendo un módulo lógico de gestión de los datos, la utilización de una tarjeta con chip ofrece varias ventajas. Permite reducir los costes de realización del dispositivo, siendo hoy en día la fabricación de la tarjeta con chip una fabricación en masa. Permite igualmente aprovechar los medios de seguridad intrínseca integrados en todas las tarjetas con chip. La modificación fraudulenta de tal tarjeta es difícil. Permite igualmente disponer de periféricos disponibles para programar las tarjetas y, por lo tanto, para generar fácilmente dispositivos programados con derechos particulares según los usos. Pueden igualmente y de una manera fácil re-utilizar la tarjeta mediante una simple programación de los derechos para re-distribuirla. Puede igualmente ser distribuida bajo la forma de una ficha que permite más de un acceso a la red.

La tarjeta con chip 2.1 está dotada con un módulo de radio de conexión Wi-Fi 2.2. Gracias a este módulo de radio, la tarjeta misma puede establecer conexiones Wi-Fi físicas con un punto de acceso. Alternativamente, este módulo de radio puede ser implementado en un lector de tarjetas y comunicarse con éste. La tarjeta con chip está controlada por un microcontrolador o procesador 2.3. Posee un conjunto lógico compuesto de un sistema de explotación y de un conjunto de aplicaciones alojadas en la memoria muerta o ROM 2.4. Estas lógicas utilizan la memoria viva 2.5 para su ejecución. Es corriente igualmente que este tipo de tarjetas posea un co-procesador criptográfico 2.7 que es permita acelerar las operaciones de cifrado utilizadas tanto para la autentificación como para un eventual cifrado de los datos transmitidos. Finalmente, la tarjeta con un chip posee un módulo de gestión de las entradas/salidas 2.6 que genera los accesos desde el exterior y en este caso con el lector de tarjetas 2.10. Todos estos módulos se comunican con la ayuda de un bus 2.8.

Los intercambios con el terminal al que están conectada esta tarjeta con chip pasan, en el ejemplo de realización del invento, por un lector de tarjetas 2.10 que dispone de una conexión USB 2.12 con el terminal y que genera las entradas/salidas de la tarjeta con chip 2.1 con la ayuda de la conexión 2.9, haciéndose la adaptación mediante el módulo de adaptación 2.11.

Cuando el dispositivo está conectado al terminal, parece como un interfaz de red de éste. Recupera entonces una dirección IP en concordancia con la red a la cual está conectado. Para permitir la comunicación en TCP/IP por encima de la conexión USB, la elección está soportada por la utilización del protocolo RNDIS (Remote Network Driver Inteface Specification, desarrollada por Microsoft). Se trata de una especificación para periféricos de red que funcionan en un bus como, por ejemplo, USB. Esta elección permite ser compatible sin necesitar parametraje alguno o añadir una lógica particular con una amplia selección de sistemas de explotación del terminal del usuario tales como Windows Vista, Apple Mac OS X o Linux, que integran en su distribución por defecto la gestión RNDIS. En Windows XP, es sencillamente necesario añadir un fichero “. Inf” de algunos kilo-octetes. Esta elección permite, por lo tanto, la utilización sencilla del dispositivo según el invento con la mayor parte de las terminales de los usuarios disponibles en el mercado. El experto comprende que se pueden hacer otras elecciones sobre este punto, y de una manera más particular si el invento se realiza con una conexión distinta que USB entre el dispositivo y el terminal.

La parte del dispositivo de tarjeta con chip no está obligada a interpretar IP para funcionar limitando la utilización en el espacio y en el tiempo. Por el contrario, si las restricciones de acceso a ciertos lugares- por ejemplo, no se quiere autorizar el acceso a una dirección IP precisa- no se hacen por el punto de acceso sino por el dispositivo, la parte de tarjeta con chip puede interpretar IP y prohibir cualquier conexión con las direcciones IP prohibidas. Pueden establecerse otras restricciones: la tarjeta puede interpretar otros protocolos y de esta manera, controlarlos, por ejemplo, la interpretación de DNS (Domain Name Server, en inglés) permite prohibir nombres de dominios. Los derechos de acceso son generados por la parte de tarjeta con chip. El usuario que utilice el dispositivo no tiene ningún control sobre los derechos de acceso concedidos y no puede modificarlos.

Un módulo de gestión de los derechos de acceso a la red sin hilos está implementado en la tarjeta. Este módulo está integrado de una manera ventajosa en el piloto del módulo de radio 2.2 que genera el acceso a Wi-Fi. Cuando el usuario del terminal desea activar una conexión con la red de comunicación, solicita esta activación de conexión al dispositivo. Esta solicitud de la activación puede tomar diversas formas según los modos de realización del invento. Según un primer modo de realización, al estar enganchado el dispositivo al ordenador huésped, la solicitud se efectúa mediante una acción del usuario sobre este ordenador huésped. Esta acción puede hacerse por intermedio de una lógica dedicada a la gestión del dispositivo o por intermedio de los utilitarios de gestión de la red integradas en el sistema de explotación. Esta acción desencadena entonces la activación del dispositivo. Según otro modo de

realización, el dispositivo dispone de un órgano de control, botón u otro sistema, que permite al usuario activas la conexión. Según otro modo más de realización, la activación de la conexión es automática durante el enganche del dispositivo a la máquina huésped. En este caso, el usuario solicita la activación de la conexión simplemente enganchando el dispositivo. Esta solicitud de la activación es tratada por el piloto del módulo de radio 2.2. La solicitud se genera entonces por el módulo de gestión de los derechos de acceso que va a verificar si se reúnen un conjunto de condiciones relacionadas con estos derechos para autorizare o no la conexión.

Estos derechos de acceso son almacenados de una manera ventajosa en la memoria protegida, es decir, en una memoria de la tarjeta con chip que no es accesible desde el exterior excepto con la ayuda de un útil de programación ad hoc. Estos derechos incluyen una referencia de la red sin hilos a la cual está asociado el dispositivo, típicamente una identificadora SSID (Service Set Identifier, en inglés), de la red en el caso de Wi-Fi. De una manera ventajosa, pueden incluir igualmente un umbral de la fuerza de la señal como elemento potencial de control geográfico. De una manera ventajosa, incluyen igualmente la clave de cifrado, por ejemplo, una clave WPA (Wi-Fi Protected Access, en inglés), WPA2, WPA-Entreprise o WPA2-Entreprise, utilizada para el cifrado de los intercambios sin hilos entre el dispositivo y el punto de acceso. Algunas de estas claves pueden estar bajo la forma de unos certificados que permiten limitar en el tiempo la utilización de esta clave. Incluyen igualmente unos identificadores de la conexión a la red, típicamente un nombre de conexión (login, en inglés) y una palabra de paso, pero pude utilizarse cualquier otro tipo de identificador. Cualquier tipo de política de gestión de los derechos de acceso puede utilizarse acompañado de unos parámetros asociados. Por ejemplo, en el caso de un acceso limitado en el tiempo, se almacena el resto del tiempo disponible, o crédito de tiempo, asociado a la tarjeta. En el caso de un acceso limitado geográficamente, se almacenan los identificadores del punto de acceso o de los puntos de acceso autorizados, así como, eventualmente, los umbrales de la fuerza de la señal requerida.

La Figura 3 ilustra un ejemplo de funcionamiento del módulo de gestión de los derechos de acceso en el caso de una limitación temporal del acceso. Durante una etapa 3.1, el módulo recibe una solicitud de activación de la conexión. Comprueba entonces si queda tiempo disponible, es decir, si queda crédito del tiempo concedido al dispositivo durante una etapa 3.2. Comprueba igualmente, no siendo significativo el orden de estos tests, si la red a la que está asociado está disponible durante una etapa 3.3. Este test de disponibilidad puede incluir igualmente el test eventual del hecho de que la fuerza de la señal sea superior a una fuerza de la señal requerida. Si uno de estos tests es negativo, el dispositivo se niega a establecer la conexión durante la etapa 3.8. Si estos dos tests dos positivos, el dispositivo se autentifica al punto de acceso durante la etapa 3.4, y conseguida esta autentificación, establece una conexión con el punto de acceso durante una etapa 3.5. Mientras que permanece establecida la conexión, el módulo efectúa un descuento del tiempo durante una etapa 3.6. Para ello, comprueba periódicamente si queda tiempo disponible, etapa 3.7. El descuento del tiempo puede hacerse, por ejemplo, con la ayuda de un reloj interno en el token. El tiempo que queda se descuenta hasta la desconexión del token. En el caso de la utilización de un certificado, la fecha de validez se verifica mediante el interrogatorio de un servidor de tiempos que utiliza el protocolo NTP (Network time Protocol, en inglés) para conocer la fecha actual precisa. A continuación, el reloj interno se utiliza para conocer la hora actual y asegurarse que el certificado no llega a su expiración. Es posible pensar en un dispositivo que combine la utilización del descuento del tiempo y un certificado (puede hacerse un paralelismo con un forfait telefónico en un límite de tiempo (1 hora) a utilizar durante 1 mes). En el caso de la utilización de un certificado, el límite de acceso es un límite representado por una fecha fijada, la fecha de revocación del certificado, más allá de la cual la conexión no será posible. El límite es, entonces, independiente del tiempo de conexión. La hora actual se compara periódicamente con la fecha y la hora de la revocación del certificado con el fin de verificar la validez. El servidor NTP puede ser implementado en la red local, pero también es posible utilizar los servidores disponibles en la red de comunicación a la cual se accede. Típicamente, tales servidores están disponibles en la red de Internet. Cuando el límite del tiempo concedido alcanza el valor nulo o cuando el certificado llega a la expiración el dispositivo corta la conexión durante la etapa 3.8.

Alternativamente, el punto de acceso puede ser programado para verificar la validez del certificado con el fin de autorizar o no la conexión. En esta alternativa, es el punto de acceso el que se ocupa de prohibir la conexión una vez que la fecha de validez del certificado se ha sobrepasado.

La Figura 4 ilustra otro ejemplo de funcionamiento de un dispositivo según el invento en el caso de una gestión de los derechos de acceso por una limitación geográfica. Se encuentra una etapa 4.1 de recepción de una solicitud de activación de la conexión. En este caso, el dispositivo dispone de una lista eventualmente unitaria de los identificadores de los puntos de acceso autorizados para una conexión a partir de este dispositivo. Estos identificadores pueden, especialmente, contener el nombre de la red (ESSID), la dirección MAC del punto de acceso (SSID), la dirección IP del punto de acceso e incluso igualmente la fuerza de la señal requerida. La utilización de esta fuerza de la señal requerida permite limitar el acceso a una zona geográfica próxima al punto de acceso. Esta lista está configurada en el dispositivo durante su personalización. El módulo de gestión comprueba entonces durante una etapa 4.2 los puntos de acceso disponibles, es decir los que se encuentran al alcance radio. Verifica si al menos uno de estos puntos es un punto de acceso autorizado durante una etapa 4.3. Este test incluye la verificación eventual de que la fuerza de la señal es al menos igual a la fuerza de la señal requerida. Si este test es negativo, la conexión es denegada en una etapa 4.6. Si este test es positivo, el dispositivo se autentifica en un punto de acceso durante una etapa 4.4. Después de conseguida la autentificación, se establece la conexión durante una etapa 4.5 con el punto de acceso autorizado detectado.

De una manera ventajosa, se añade una etapa de autentificación del usuario en el dispositivo. En algunos casos, esta seguridad suplementaria puede resultar útil. Esta etapa puede hacerse de varias maneras. Lo más seguro es dotar al dispositivo de un detector biométrico que permita la identificación, por ejemplo, por medio de un dispositivo de reconocimiento de la huella digital ejecutada por el dispositivo (Match On Card o MOC, en inglés). Debido a esto, ninguna entrada relativa a la autentificación se hace en el terminal del cliente y no es, por lo tanto, susceptible de ser capturada por una lógica malvada. Alternativamente, puede hacerse una autentificación por una palabra de pase. En este caso, el usuario abre un navegador WEB, por ejemplo, en el terminal y se conecta al dispositivo. El dispositivo posee un servidor WEB embarcado que propone una página de autentificación. Observemos que esta última solución impone la implementación de IP, HTTP, TLS y TCP en la parte de la tarjeta.

Los derechos de acceso pueden ser definidos, de igual manera, bajo la forma de una lista de control del acceso ACL (Access Control List, en inglés) configurada durante la fase de personalización del dispositivo. Esta ACL determina qué conexiones están autorizadas. Las cuales deben ser aseguradas por parte del dispositivo y las cuales no tienen ninguna razón para serlo. Es posible, entonces, generar unas autorizaciones al nivel de los servicios distantes accesibles, para autorizar algunas y prohibir otras. El dispositivo juega entonces el papel de un apaga-fuegos que filtra el tráfico de una manera selectiva. Es posible, de igual manera, integrar un sistema de túnel cifrado o VPN (Virtual Private Network, en inglés) y, no autorizar, por lo tanto, nada más que la conexión a una red distante particular a través de este túnel, quedando inaccesible el resto.

La personalización del dispositivo puede hacerse, por ejemplo, por unos medios habituales de programación de una tarjeta con un chip segura. Esta personalización necesita unas autorizaciones que permitan garantizar que un usuario no pueda modificar los derechos programados en el dispositivo.

Tal dispositivo ofrece la ventaja de conservar las informaciones sensibles en el dispositivo, protegidas de una manera ventajosa en el seno de una tarjeta con un chip. Permite la utilización de la red sin hilos sin ninguna modificación de la red. El terminal puede utilizarla como un periférico de una red clásica.

REIVINDICACIONES

1.Dispositivo de acceso a una red sin hilos que incluye:

-unos medios de conexión a un dispositivo huésped;

- unos medios de conexión a un punto de acceso de una red sin hilos;

- unos medios para abrir una conexión con el punto de acceso a la red sin hilos a la recepción de una solicitud de activación de la conexión de tal forma que permita el acceso a la red sin hilos a la máquina huésped a la cual está conectado;

caracterizado por que incluye, además:

-unos medios de gestión de los derechos de acceso a la red sin hilos para verificar los derechos de acceso antes de abrir la conexión.

2. Dispositivo según la reivindicación 1, caracterizado por que al menos los medios de gestión de acceso a la red sin hilos están integrados en una tarjeta con un chip.

3. Dispositivo según una de las reivindicaciones 1 ó 2, caracterizado por que los medios de gestión de acceso a la red sin hilos incluyen unos medios para limitar temporalmente este acceso.

4. Dispositivo según la reivindicación 3, caracterizado por que los medios de gestión de los derechos de acceso a la red sin hilos incluyen un certificado que tiene una duración de validez restringida.

5. Dispositivo según la reivindicación 3, caracterizado por que los medios de gestión de los derechos de acceso a la red sin hilos incluyen unos medios para descontar el tiempo de conexión de un crédito programado.

6. Dispositivo según una de las reivindicaciones 1 ó 2, caracterizado pir que los medios de gestión de los derechos de acceso a la red sin hilos incluyen unos medios para limitar geográficamente este acceso.

7. Dispositivo según una de las reivindicaciones 1 ó 2, caracterizado por que los medios de gestión del acceso a la red sin hilos incluyen unos medios de gestión de unas listas de control de acceso que permiten determinar cuáles conexiones están autorizadas.

8. Procedimiento de gestión de los derechos de acceso a una red sin hilos caracterizado por que incluye las siguientes etapas efectuadas por un dispositivo de acceso a la red sin hilos:

-una etapa de recepción de una solicitud de activación de la conexión por parte del dispositivo de acceso a la red sin hilos que incluye unos medios de conexión a un dispositivo huésped, unos medios de conexión a un punto de acceso a una red sin hilos y unos medios para abrir una conexión con el punto de acceso de la red sin hilos a la recepción de una solicitud de activación de la conexión de tal manera que permita el acceso a la red sin hilos a la máquina huésped a la que está conectado:

- una etapa de test, incluyendo la etapa de test:

- una etapa de test de los puntos de acceso disponibles y una etapa de verificación de que al menos un punto de acceso disponible está autorizado;

o bien,

-una etapa de test del tiempo disponible y una etapa de test de la disponibilidad de la red:

- una etapa de conexión si este test es positivo,

- una etapa negando la conexión si este test es negativo.

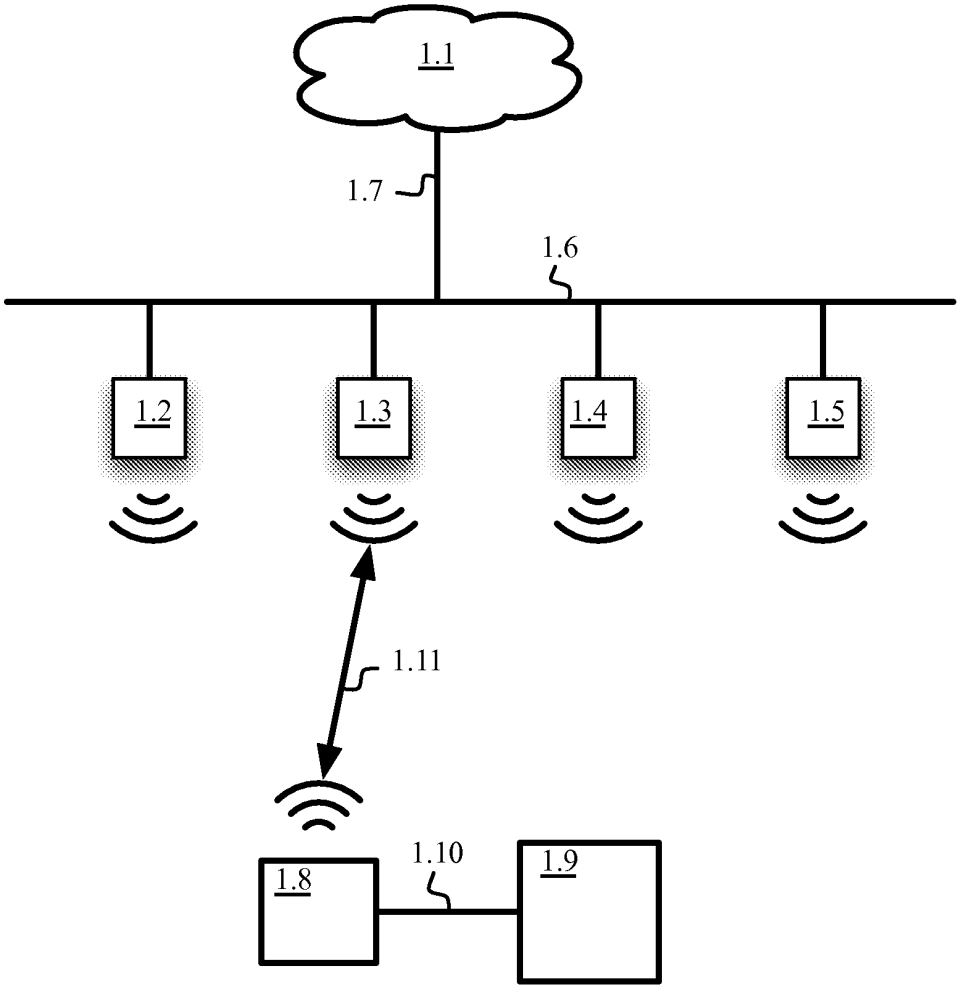

Fig. 1

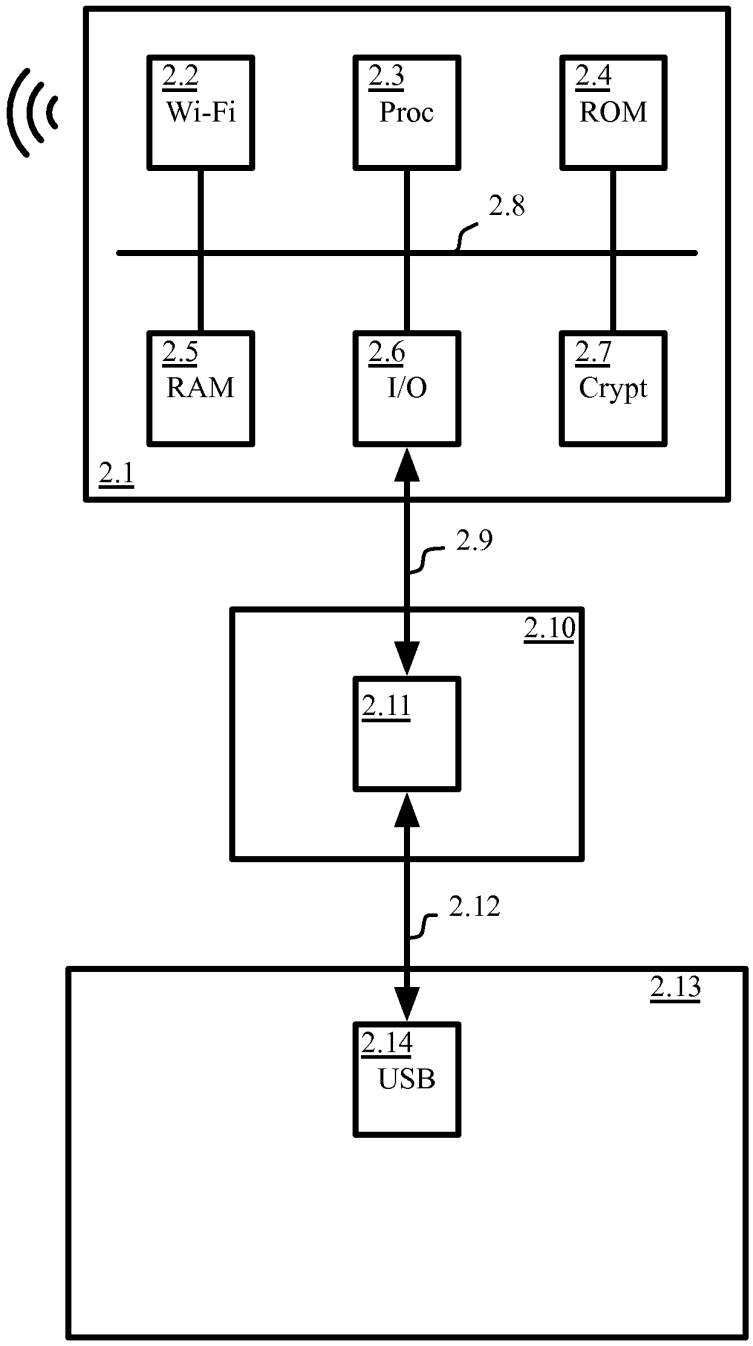
2.2
Wi-Fi
2.3
Proc
2.4
ROM
2.8
2.5
RAM
2.6
I/O
2.7
Crypt
2.1
2.9
2.10
2.11
2.12
2.13
2.14
USB

Fig. 2

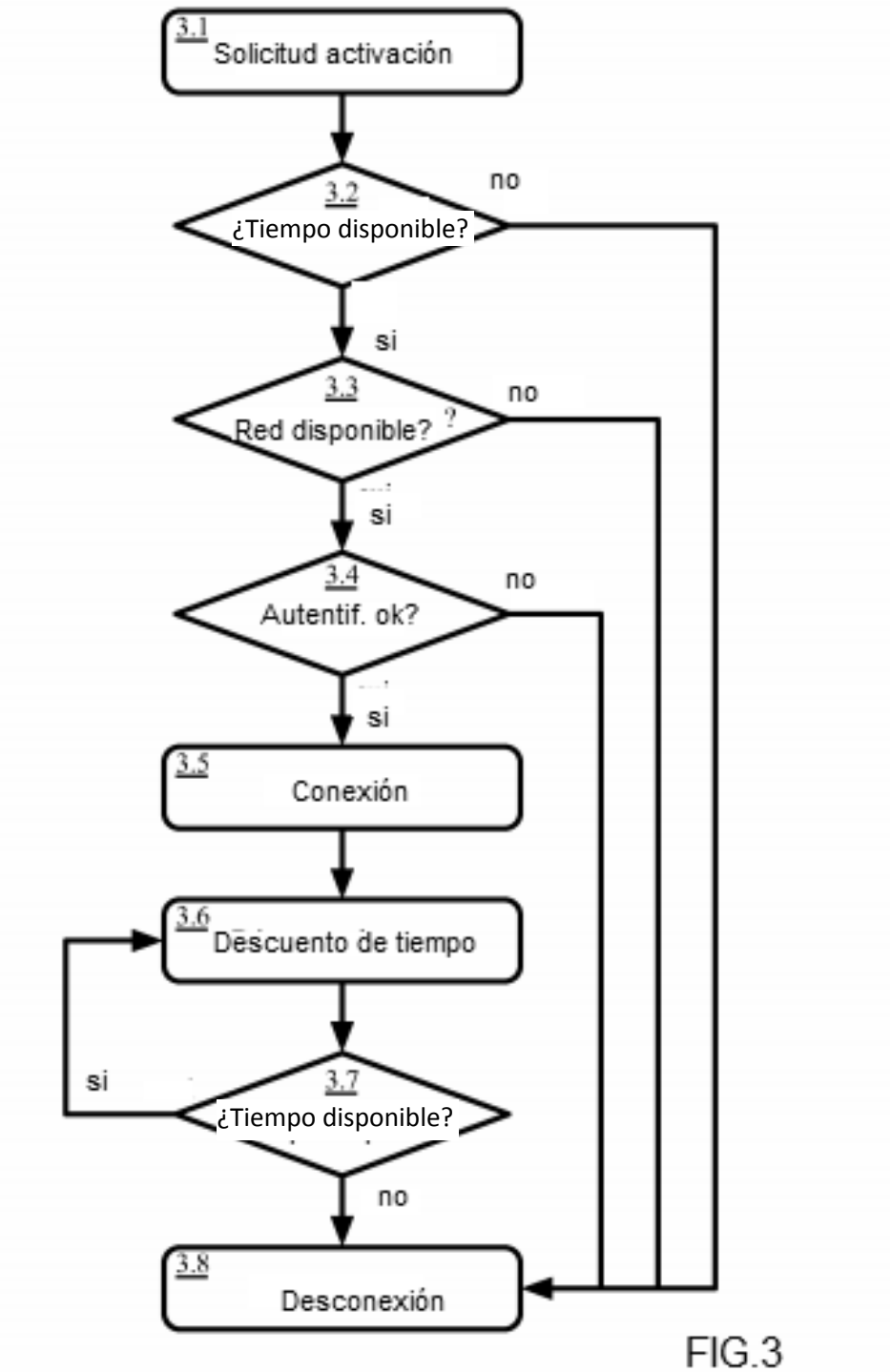
3.1
Solicitud activación
3.2
¿Tiempo disponible?
no
si
3.3
Red disponible?
no
si
3.4
Autentif. ok?
no
si
3.5
Conexión
3.6
Descuento de tiempo
si
3.7
¿Tiempo disponible?
no
3.8
Desconexión

FIG.3

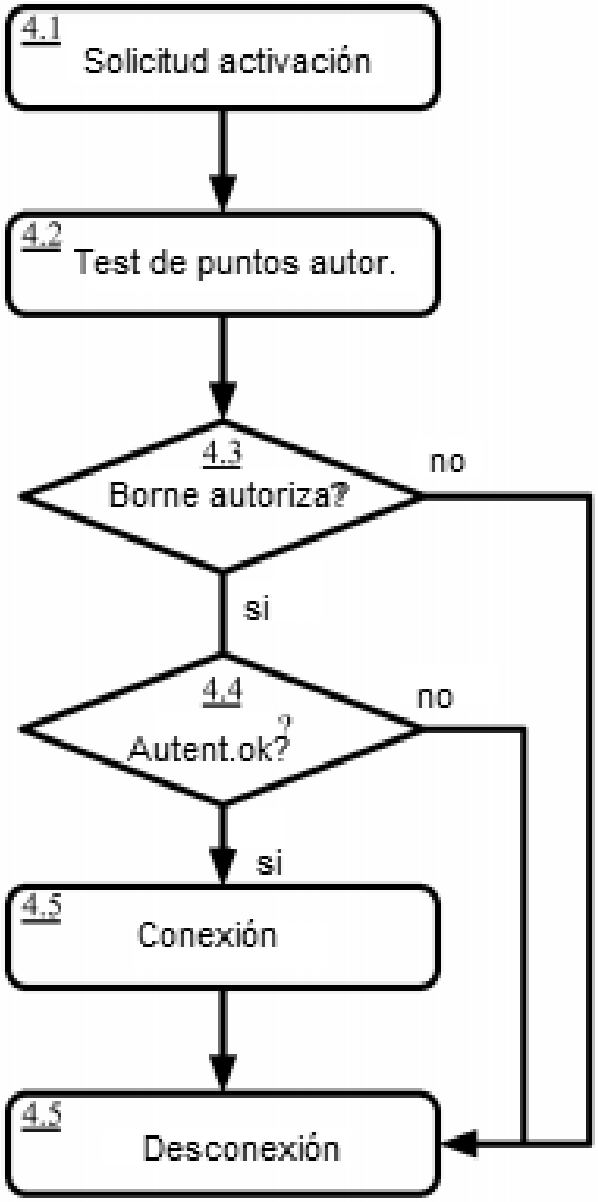
4.1
Solicitud activación
4.2
Test de puntos autor.
4.3
Borne autoriza?
no
si
4.4
Autent.ok?
no
si
4.5
Conexión
4.5
Desconexión

Fig. 4