(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 328 607**

(51) Int. Cl.:
H04L 12/56 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05801039 .8**
(96) Fecha de presentación : **09.09.2005**
(97) Número de publicación de la solicitud: **1790136**
(97) Fecha de publicación de la solicitud: **30.05.2007**

(54) Título: **Adaptador USB para red inalámbrica con tarjeta de chip.**

(30) Prioridad: **15.09.2004 EP 04292215**

(45) Fecha de publicación de la mención BOPI:
16.11.2009

(45) Fecha de la publicación del folleto de la patente:
16.11.2009

(73) Titular/es: **Gemalto S.A.**
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es: **Danre, Nicolas**

(74) Agente: **Cañadell Isern, Roberto**

DESCRIPCIÓN

Adaptador USB para red inalámbrica con tarjeta de chip.

La presente invención se refiere en general a los aspectos de seguridad del trabajo en redes inalámbricas, también conocido como fidelidad inalámbrica o "Wi-Fi" (wireless fidelity), y más concretamente a un adaptador USB para red inalámbrica que ofrece una funcionalidad de alta seguridad y fácil manejo.

Las redes inalámbricas de ordenadores están muy extendidas hoy en día. Son especialmente útiles para facilitar el acceso a la red de los ordenadores portátiles, que se pueden conectar temporalmente a la red sin necesidad de enchufar un cable entre un concentrador de red y el ordenador.

Una red inalámbrica consta de un punto de acceso y ordenadores cliente que pueden conectarse a la red con ayuda de hardware cliente, el denominado "adaptador de red", que establece una conexión por radio con el punto de acceso. Estos adaptadores de red se pueden integrar en el ordenador por medio de tarjetas de red o bien pueden ser dispositivos externos que se conectan al ordenador, por ejemplo a través de la interfaz USB (adaptador USB para red inalámbrica).

El bus serie universal USB (universal serial bus) es una interfaz normalizada que incorporan prácticamente todos los ordenadores personales fabricados desde 1997. Los dispositivos USB se enchufan al puerto USB del ordenador a través de un sencillo conector. Muchos dispositivos USB, incluidos los adaptadores para red inalámbrica, se fabrican en forma de "tokens" o llaves USB, que es un dispositivo portátil tan pequeño (de 5 a 10 cm de largo y 1 o 2 cm de ancho) que se puede llevar fácilmente en un llavero. Esto es ideal para las personas que viajan llevando consigo un portátil.

Véase la patente US 2004/0 068 653 (Fascenda) que divulga un acceso a red compartido utilizando diferentes llaves de acceso.

Dado que el acceso a las redes inalámbricas es posible para cualquier persona que esté en el radioalcance del punto de acceso, estas redes están muy expuestas a sufrir ataques contra su seguridad. Estos ataques pueden ir desde el simple uso gratuito de la red, por ejemplo para obtener acceso a Internet, hasta espiar, modificar o borrar datos almacenados en los ordenadores conectados a la red.

Es posible conseguir un alto nivel de seguridad utilizando credenciales de autenticación únicas para cada usuario y que estos deberán conservar. Por ejemplo, en una infraestructura de clave pública o PKI (public key infrastructure), los usuarios poseen una clave privada secreta con la que pueden autenticarse y en la arquitectura telefónica GSM, los usuarios se autentican por medio de un identificador único validado por una clave secreta. Antes de permitir el acceso, se ejecuta un proceso de pregunta/respuesta entre el dispositivo que solicita el acceso y la red inalámbrica. Durante este proceso de pregunta/respuesta, se garantiza la seguridad con algoritmos que utilizan credenciales de autenticación y elementos generados de forma aleatoria para cada proceso.

Almacenar credenciales de autenticación en los discos duros de los ordenadores es un sistema ineficaz y peligroso. Los discos duros pueden averiarse y de hecho se averían, y las credenciales pueden ser robadas (copiadas) sin que el usuario se entere siquiera de que se ha comprometido su seguridad. Por esta razón, es más seguro integrar las credenciales en un elemento físico con capacidad criptográfica, que ofrezca una fuerte protección.

Una posibilidad para ofrecer un alto nivel de seguridad de acceso a las redes inalámbricas sería integrar las credenciales del usuario en el adaptador de red utilizado. Por desgracia, aunque estos elementos físicos podrían admitir la generación de claves internamente, no se pueden personalizar en masa, lo que implica que los usuarios finales tienen que introducir las credenciales manualmente, una por una. Además, para que las prestaciones de seguridad personalizada se adapten a una o varias arquitecturas o utilicen algoritmos personalizados, habría que diseñar adaptadores de red específicos.

Por el contrario, las tarjetas inteligentes resultan ideales para almacenar credenciales de alto valor. Se trata de un medio que ofrece máxima protección contra manipulaciones, capaz de procesar algoritmos seguros y que además se puede personalizar en masa de forma económica. Una tarjeta inteligente puede conectarse al ordenador a través de un lector de tarjetas inteligentes, que a su vez se conecta al ordenador por ejemplo a través de la interfaz USB. Desde hace poco, el solicitante comercializa tarjetas inteligentes con el nombre de producto "e-gate", donde el protocolo USB se implanta incluso en la propia tarjeta inteligente, de manera que se pueda enchufar ésta directamente al puerto USB del ordenador a través de un sencillo conector. Este conector no lleva ningún componente electrónico, a diferencia de un lector para tarjetas inteligentes tradicional, que sólo admite los protocolos de comunicación estándar de la ISO (Organización Internacional de Normalización).

Sin embargo, pese a todas las ventajas que conlleva el uso de tarjetas inteligentes para almacenar credenciales de autenticación y otros datos que afectan a la seguridad, el empleo de una tarjeta inteligente para la gestión de la seguridad además del adaptador para red inalámbrica para facilitar el acceso a la red tiene la desventaja de que el despliegue de todo el hardware y software necesario para obtener acceso seguro a la red se divide en dos tareas totalmente independientes: (1) la instalación del adaptador para red inalámbrica; y (2) la instalación de los dispositivos relacionados con la seguridad, como por ejemplo una tarjeta inteligente que almacene credenciales de autenticación. Este proceso de instalación en dos fases no es fácil de manejar para el usuario y, sobre todo si los dos dispositivos son

de fabricantes diferentes, pueden producirse problemas de interoperabilidad entre ambos dispositivos. En la técnica convencional, no existe ninguna solución que combine las dos fases de instalación en una sola.

Por consiguiente, el objeto de la invención es proporcionar un dispositivo que resuelva los problemas anteriormente descritos. Este objeto se consigue por medio de los dispositivos definidos en las reivindicaciones independientes 1 y 6. En las reivindicaciones dependientes se definen realizaciones preferidas adicionales.

En una realización preferida de la invención, el objeto de la misma se consigue por medio de un dispositivo capaz de comunicarse con un ordenador a través de una interfaz USB, comprendiendo el dispositivo un concentrador USB y un adaptador USB para red inalámbrica que se conecta al concentrador USB, y estando adaptado de tal manera que se pueda conectar al concentrador USB una tarjeta inteligente capaz de comunicarse con el protocolo USB.

Equipar un adaptador de red con una tarjeta inteligente, combinando ambos en un solo dispositivo, tiene la ventaja de que no es necesario instalar dos dispositivos independientes para facilitar el acceso seguro a las redes inalámbricas. Además, sólo hace falta dedicar un único puerto USB del ordenador a las dos funcionalidades. Más aún, se facilita la personalización en masa del dispositivo combinado. Dado que la tarjeta inteligente de la invención puede comunicarse con el protocolo USB, puede utilizarse un sencillo concentrador USB para conectar tanto el adaptador de red como la tarjeta inteligente al ordenador.

En otra realización preferida de la invención, el dispositivo es una llave USB portátil.

Las llaves USB son pequeñas, manejables y fáciles de llevar y, por lo tanto, son muy populares entre los usuarios.

En otra realización preferida de la invención, la tarjeta inteligente que se va a conectar al concentrador USB puede insertarse en el dispositivo.

Por lo tanto, el dispositivo ofrece una sola carcasa para el adaptador de red y la tarjeta inteligente. No requiere conexión a través de un cable externo o similar.

En otra realización preferida de la invención, el dispositivo comprende además la tarjeta inteligente, que se conecta al concentrador USB.

En esta realización de la invención, el dispositivo se entrega con la tarjeta inteligente ya insertada en el mismo, de manera que el usuario no tiene que insertar la tarjeta inteligente.

En otra realización preferida de la invención, todas las operaciones que tienen que ver con la gestión de la seguridad del acceso a la red se delegan en la tarjeta inteligente, que se conecta al concentrador USB.

Dado que la tarjeta inteligente ofrece máxima protección contra manipulaciones, se considera el mejor lugar para almacenar credenciales de autenticación secretas y gestionar otros aspectos de seguridad del acceso a la red.

Otra realización preferida de la invención es una tarjeta inteligente capaz de comunicarse con el protocolo USB, estando adaptada dicha tarjeta inteligente para utilizarse conjuntamente con uno de los dispositivos anteriormente descritos.

En otra realización preferida de la invención, la tarjeta inteligente almacena credenciales de autenticación de forma segura. Como se ha explicado anteriormente, la tarjeta inteligente es el lugar ideal para almacenar información crítica, como credenciales de autenticación.

La tarjeta inteligente también puede personalizarse con algoritmos específicos y puede encargarse de parte o la totalidad del proceso de pregunta/respuesta de autenticación.

La tarjeta inteligente también puede almacenar múltiples credenciales de autenticación para poder identificarse en dos o más redes inalámbricas que utilicen una arquitectura de seguridad diferente.

Todo lo anterior y otros objetos, aspectos y ventajas de la invención se entenderán mejor en la siguiente descripción detallada de una realización preferida de la invención realizada con referencia al dibujo, donde:

Fig. 1 es un esquema que representa la arquitectura de una realización preferida de la invención.

En referencia a los dibujos, la Figura 1 representa la arquitectura de una realización preferida de la invención, que consiste en un dispositivo integrado por un adaptador USB para red inalámbrica 2 y una tarjeta inteligente 3 capaces de comunicarse con el protocolo USB. Dado que tanto el adaptador 2 como la tarjeta 3 están habilitados por USB, pueden conectarse a un concentrador USB 1. El concentrador 1 puede conectarse al ordenador a través de una conexión USB, es decir, el dispositivo puede enchufarse a un puerto USB del ordenador. A través del concentrador, tanto el adaptador 2 como la tarjeta 3 se conectan al ordenador. Obsérvese que el dispositivo de la invención no tiene por qué incluir necesariamente la tarjeta 3 propiamente dicha, sino que ha de proporcionar los medios para conectar una tarjeta inteligente habilitada por USB a su concentrador USB 1.

Dado que las dimensiones físicas y la colocación de los conectores de los chips de la tarjeta vienen especificadas por las normas ISO, el hardware que constituye la interfaz física con la tarjeta inteligente ha de cumplir dichas normas. Por ejemplo, en una realización de la invención donde la tarjeta inteligente 3 puede insertarse en el dispositivo (es decir, puede colocarse dentro de la carcasa del dispositivo), éste comprende los medios para retener la tarjeta 3 y la interfaz física (por ejemplo, los contactos electrónicos) para acceder a la tarjeta inteligente, ajustándose la interfaz física a las normas ISO.

Pero dado que el protocolo USB está implantado en la tarjeta inteligente 3, las normas ISO aplicables al protocolo de comunicación entre la tarjeta y el lector de tarjetas no tienen por que aplicarse al dispositivo, ni tiene el dispositivo que disponer de medios para traducir los protocolos de comunicación ISO al protocolo USB.

El dispositivo de la invención estará diseñado en general de manera que la tarjeta inteligente 3 pueda ser insertada y extraída del dispositivo, como es el caso del factor de forma "token" del producto "e-gate" del solicitante antes mencionado. En este caso, los fabricantes pueden optar por entregar el dispositivo con o sin tarjeta inteligente. Sin embargo, la tarjeta 3 también podría estar integrada de forma fija en el dispositivo.

En general, el dispositivo será una llave USB, del tamaño de los adaptadores USB convencionales para red inalámbrica en el factor de forma "token".

A partir de aquí es posible delegar de forma ventajosa todas las operaciones que tienen que ver con la gestión de la seguridad en la tarjeta inteligente 3, especialmente lo que respecta a los problemas de seguridad del acceso a la red inalámbrica. Por ejemplo, en la tarjeta inteligente se pueden almacenar credenciales de autorización como claves privadas o certificados y la tarjeta inteligente puede manejar todo el proceso de autenticación cuando el ordenador vaya a conectarse a la red inalámbrica.

A continuación, se ofrecen tres casos de uso de la presente invención a modo de ejemplos.

(1) *Red inalámbrica corporativa*

Gracias a la invención, la empresa podrá entregar llaves "token" a sus empleados y distribuir tarjetas personalizadas con su sistema interno de gestión de tarjetas.

Pese al hecho de que cada vez son más los ordenadores personales que cuentan actualmente con adaptadores de red inalámbrica integrados, la distribución de llaves "token" puede ser muy interesante para las empresas porque reduce la necesidad de prestar asistencia a un único tipo de dispositivo.

(2) *Oferta masiva al mercado*

Gracias a la invención, un proveedor de servicios de Internet Wi-Fi (zona de cobertura o "hot spot") puede entregar llaves "token" a sus clientes, junto con tarjetas inteligentes que hayan sido personalizadas por un centro de personalización. El centro de personalización gestionará las credenciales de autenticación y las almacenará en las tarjetas utilizando la información del cliente facilitada por el proveedor de servicios de Internet. El cliente podrá entonces autenticarse con la llave "token" en cualquier ordenador de cualquier punto de acceso desplegado por el proveedor de servicios de Internet Wi-Fi.

(3) *Un proveedor de servicios de Internet por ADSL proporciona enrutadores o "routers" ADSL inalámbricos seguros*

Gracias a la invención, el proveedor de servicios de Internet por ADSL puede proporcionar un router ADSL con llaves "token" para sus clientes, y tarjetas inteligentes específicamente personalizadas para conectarse únicamente a este router en concreto o a los routers proporcionados por el proveedor de servicios.

REIVINDICACIONES

1. Un dispositivo capaz de comunicarse con un ordenador a través de una interfaz USB, comprendiendo dicho dispositivo un concentrador USB (1) y estando adaptado de manera que se pueda conectar una tarjeta inteligente (3), capaz de comunicarse con el protocolo USB, al concentrador USB (1), donde el dispositivo comprende un adaptador USB para red inalámbrica (2) que se conecta al concentrador USB (1).

2. Dispositivo conforme a la reivindicación 1, donde dicho dispositivo es una llave USB portátil.

3. Dispositivo conforme a las reivindicaciones 1 ó 2, donde la tarjeta inteligente que se va a conectar al concentrador USB (1) se puede insertar en el dispositivo.

4. Dispositivo conforme a una de las reivindicaciones anteriores, donde el citado dispositivo comprende además la tarjeta inteligente (3) que se conecta al concentrador USB (1).

5. Dispositivo conforme a una de las reivindicaciones anteriores, donde todas las operaciones que tienen que ver con la gestión de la seguridad del acceso a la red se delegan en la tarjeta inteligente (3), que se conecta al concentrador USB (1).

6. Tarjeta inteligente (3) capaz de comunicarse con el protocolo USB, estando adaptada dicha tarjeta (3) para utilizarse conjuntamente con un dispositivo conforme a las reivindicaciones 1 a 5.

7. Tarjeta inteligente (3) conforme a la reivindicación 6, donde dicha tarjeta almacena credenciales de autenticación de forma segura.

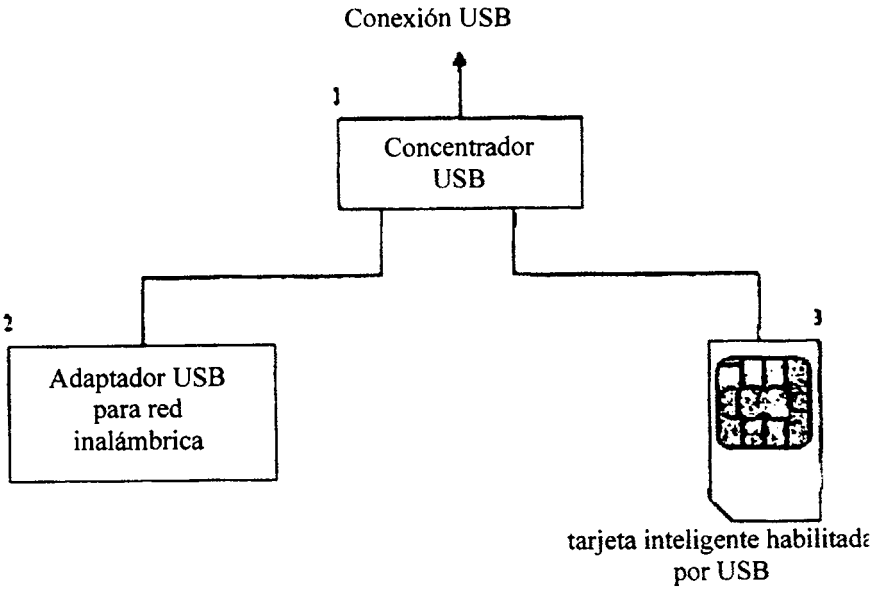
Conexión USB
1
Concentrador USB
2
Adaptador USB para red inalámbrica
3
tarjeta inteligente habilitada por USB

Figura 1