(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 340 043**

(51) Int. Cl.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05014926 .9**
(96) Fecha de presentación : **09.07.2005**
(97) Número de publicación de la solicitud: **1626323**
(97) Fecha de publicación de la solicitud: **15.02.2006**

(54) Título: **Control de acceso y protección contra una copia.**

(30) Prioridad: **11.08.2004 DE 10 2004 039 104**

(45) Fecha de publicación de la mención BOPI:
28.05.2010

(45) Fecha de la publicación del folleto de la patente:
28.05.2010

(73) Titular/es: **Andreas Hopp**
Hardenbergstrasse 48
45472 Mülheim a.d.R., DE
Gerhard Ostrowski y
Axel Wieskus

(72) Inventor/es: **Hopp, Andreas y**
Ostrowski, Gerhard

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Control de acceso y protección contra una copia.

La invención se refiere generalmente a un procedimiento para el control de una autorización de acceso a productos de software.

En el caso de productos de software convencionales, en particular en el caso de programas que pueden instalarse fijamente en un ordenador, hasta ahora no se ha resuelto por completo el problema de copias de los programas. Por ejemplo, es conocido proteger la instalación de software con ayuda de claves de instalación. Estas claves de instalación se adjuntan al producto como secuencias de cifras y deben ser introducidas manualmente por el usuario en el momento de la primera instalación. No obstante, esta secuencia de cifras puede copiarse sin más y puede conducir a una reproducción del software.

También es conocido el uso de la llamada técnica "dongle" (seguro electrónico). Para ello, se inserta en la interfaz paralela de un ordenador una pieza adicional, en la que está depositada una cadena de caracteres codificada. El software sólo puede ejecutarse cuando está instalado el dongle. El software lo comprueba en cada arranque, Puesto que sólo está depositado un identificador de acceso en el dongle, dado el caso, éste también puede copiarse fácilmente.

Por lo tanto, la invención tiene el objetivo de proporcionar una autorización de acceso y una protección contra copia para productos de software que sea segura y que pueda ser manejada fácilmente por el usuario.

El objetivo anteriormente indicado se consigue mediante el objeto de la reivindicación 1.

Los productos de software en el sentido de la invención pueden ser ofertas online, que pueden llamarse, por ejemplo, mediante Internet. Los ejemplos de realización de la descripción general y específica expuesta a continuación orientados a un programa que puede instalarse fijamente en un ordenador como producto de software sirven sólo como explicación y no forman parte de la invención.

Los identificadores de acceso son cadenas de caracteres que pueden ser codificadas y no codificadas. Los identificadores de acceso pueden ser protegidos por cifras de sumas de comprobación.

Los medios de almacenamiento son intercambiables y pueden conectarse en caso necesario fácilmente con el ordenador usado. El acceso a los medios de almacenamiento puede realizarse mediante distintas interfaces, por ejemplo USB, lectores de tarjetas inteligentes, firewire, bluetooth, PS/2 u otros.

Puesto que pueden leerse en el medio de almacenamiento el primero y el segundo identificador de acceso, comprobándose con ayuda de estos dos identificadores de acceso una autorización de acceso, puede garantizarse una mayor seguridad contra copias y accesos no autorizados a contenidos online. Además, un primer identificador de acceso está asignado de forma unívoca al producto de software. Gracias a esta asignación unívoca al producto de software, el medio de almacenamiento puede asignarse a un producto de software concreto y determinado. No obstante, el medio de almacenamiento no podría usarse en un caso así con un mismo producto de software pero con otro número de serie, por lo que no podría instalarse este producto de software con este medio de almacenamiento. También sería posible que un producto de software sin un identificador de acceso correspondiente sólo pueda instalarse en un medio de almacenamiento como instalación de prueba.

Se propone que se almacenen los dos identificadores de acceso en un dispositivo de almacenamiento USB o en una tarjeta inteligente. Estos dos medios son especialmente preferibles, puesto que pueden ser manejados de forma sumamente fácil por el usuario. Además, su fabricación es económica, por lo que no resultan costes adicionales importantes para los proveedores de los productos de software por la protección contra copia propuesta.

Para mejorar aún más el control de acceso a los productos de software, se propone almacenar los identificadores de acceso de forma asignada entre sí en una base de datos central. En esta base de datos central puede almacenarse en una tabla la asignación de los identificadores de acceso correspondientes. Los "Tupel" (tuples o tuplos) que se forman así son unívocos y permiten un control comprobando si los al menos dos identificadores de acceso pertenecen uno al otro permitiendo, por lo tanto, una autorización del producto de software.

Según una primera alternativa, el producto de software es un programa que puede ser instalado en un ordenador. Esto puede ser cualquier software de aplicaciones.

En este caso es preferible que al menos un segundo identificador de acceso sea un identificador de usuario asignado de manera unívoca a un usuario. Este identificador de usuario asignado de forma unívoca a un usuario puede almacenarse en el medio de almacenamiento, por ejemplo, en el momento de la compra del producto de software. El identificador de usuario unívoco permite la asignación unívoca al usuario correspondiente. El medio de almacenamiento se confecciona, por lo tanto, de tal modo que presente tanto el identificador unívoco del producto como al identificador unívoco del usuario. Este "Tupel" (tuple o tuplo) es único y puede usarse sólo con el producto de software correspondiente.

Para garantizar otra mejora, en particular para impedir la copia de los primeros y segundos identificadores de acceso en otro medio de almacenamiento se propone también que un tercer identificador de acceso sea un identificador de hardware asignado de forma unívoca al medio de almacenamiento. En el medio de almacenamiento propiamente dicho están montados preferiblemente microchips, de los que pueden leerse secuencias de cifras unívocas. Estos microchips están cableados preferiblemente sólo de una forma única y fija con el medio de almacenamiento. Por lo tanto, pueden "casarse" entre sí tres distintos identificadores de acceso. El "Tupel" (tuple o tuplo) formado por los tres identificadores de acceso es unívoco y no puede ser copiado.

Según un ejemplo de realización preferible se propone que durante una instalación del programa en el ordenador se lean los identificadores de acceso del medio de almacenamiento y que se compruebe la autorización de acceso mediante una rutina de instalación del programa con ayuda de los identificadores de acceso. De este modo se comprueba durante la instalación del programa, por ejemplo al llamarse una rutina de instalación, la autorización de acceso al programa. Para ello, se leen los identificadores de acceso del medio de almacenamiento y se comprueban en la rutina de instalación. Esto puede hacerse, por ejemplo, porque en los identificadores de acceso están codificadas cifras de comprobación, que se comprueban con ayuda de programas adecuados en la rutina de instalación. Sólo si las cifras de comprobación son correctas y/o si se han realizado otros procedimientos de comprobación posibles, el programa puede ser instalado. En otro caso es posible que se instale sólo una versión de prueba, que permita sólo un servicio limitado tanto en el tiempo como eventualmente en cuanto al alcance de las funciones.

Para conseguir independencia del medio de almacenamiento se propone según unas configuraciones ventajosas que se almacene al menos el identificador de usuario leído en el ordenador. Para ello, la información correspondiente puede depositarse, por ejemplo, en una entrada de "registro". Al activarse el programa puede leerse adicionalmente el identificador de hardware del medio de almacenamiento. En este caso, la presencia del medio de almacenamiento es necesaria para realizar la activación con éxito. No obstante, el almacenamiento en el ordenador no es necesario, puesto que los identificadores de acceso pueden leerse del medio de almacenamiento.

Para la autorización definitiva del programa o para la activación de otras funciones, así como para el registro del usuario se propone que tras una instalación del programa se realice una comprobación del identificador de acceso mediante una red de datos. Para ello se transmiten según unas configuraciones ventajosas los identificadores de acceso a través de la red de datos a un ordenador central, se comparan los identificadores de acceso transmitidos al ordenador central con identificadores de acceso almacenados en la base de datos central transmitiéndose sólo en caso de una comprobación positiva una autorización a través de la red de datos al ordenador. De este modo se permite en particular una comprobación de la asignación de los identificadores de acceso en la base de datos propiamente dicha con los identificadores de acceso recibidos. Puesto que en la base de datos existe una asignación unívoca de los al menos dos identificadores de acceso puede comprobarse inmediatamente si la combinación recibida de identificadores de acceso corresponde a un "Tupel" (tuple o tuplo) almacenado de teste tipo. Sólo en este caso es posible una autorización del programa.

Con el procedimiento según la invención también es posible vender programas protegidos o cambiar de propietario de otra manera. El uso del programa puede garantizarse en este caso porque el segundo identificador de acceso es modificado por un proveedor de tal modo que, en caso de una venta del programa, se conceda un identificador de usuario nuevo, porque el identificador de usuario nuevo se almacena junto con el identificador del producto en un medio de almacenamiento y porque el identificador de usuario nuevo se asigna al identificador del producto en la base de datos central. Un usuario nuevo puede solicitar al proveedor del programa un medio de almacenamiento nuevo. En este medio de almacenamiento nuevo se codifica el identificador de usuario unívoco y el identificador del producto. De este modo, el proveedor puede comprobar, por ejemplo, si el programa se ha vendido legalmente. También puede borrarse la asignación del identificador de usuario anterior al identificador del producto en la base de datos. El usuario anterior ya no puede usar su medio de almacenamiento para instalar el programa correctamente. Gracias al almacenamiento del identificador del usuario junto con el identificador del producto en la base de datos central, el programa puede ser activado a partir de este momento ya sólo por el usuario nuevo mediante la notificación del identificador del usuario y del identificador del producto a la base de datos central.

Según otra alternativa, el producto de software es una oferta online que puede llamarse a través de una red de datos central. Esta oferta online puede ser, por ejemplo, un servicio de correos electrónicos, un foro, una tienda online u otro servicio online.

Es preferible que en caso de un acceso a la oferta online se realice una consulta de los identificadores de acceso almacenados en el medio de almacenamiento, que los identificadores de acceso consultados sean transmitidos a través de la red de datos central a un ordenador o una red de ordenadores que gestionan la oferta online, que en la red de ordenadores se compruebe que los identificadores de acceso se correspondan unos a otros y que en caso de una comprobación positiva se realice una autorización. El usuario debe tener preparado para ello sólo el medio de almacenamiento. Esto facilita el acceso, puesto que el usuario no debe memorizar otras contraseñas.

Puede garantizarse una protección contra un acceso no autorizado porque tras haber accedido con éxito a la oferta online se modifica con ayuda del ordenador al menos el primer identificador de acceso y porque la asignación entre al menos el primero y el segundo identificador de acceso se modifica correspondientemente en la base de datos central. Aquí puede crearse mediante el ordenador o la red de ordenadores un primer identificador de acceso nuevo y transmitirse a través de la red de datos central al ordenador en el que se usa el medio de almacenamiento. En el medio de

almacenamiento es sustituido a continuación el primer identificador de acceso caducado por el identificador de acceso nuevo. Lo mismo tiene lugar en la base de datos central, en la que se modifica correspondientemente la asignación del primero y segundo identificador de acceso. A continuación, ya sólo puede concederse el acceso a la oferta online cuando se usa el primer identificador de acceso nuevo con el segundo identificador de acceso anterior. Al usarse un primer identificador de acceso caducado, puede denegarse el acceso. Para garantizar mayor seguridad se propone que la consulta de los identificadores de acceso del medio de almacenamiento sea protegida por contraseña. De este modo, en caso de un acceso a la oferta online con ayuda de los identificadores de acceso puede consultarse en primer lugar una contraseña del usuario, de modo que sólo se leen los identificadores de acceso del medio de almacenamiento si la contraseña es correcta.

A continuación, la invención se explicará más detalladamente con ayuda de un dibujo que muestra un ejemplo de realización. En el dibujo, la única figura muestra un sistema formado por una base de datos central y un ordenador preparado para el control de acceso.

Se muestra un ordenador 2 que está conectado a través de Internet 6 con una base de datos central 4. Además, se muestra un dispositivo de almacenamiento USB 8.

En el dispositivo de almacenamiento USB 8 se almacena según una primera alternativa en el momento de la compra de un programa un identificador de producto unívoco que está asignado justamente a este programa. Además, se almacena en el dispositivo de almacenamiento USB 8 un segundo identificador de acceso como identificador de usuario. Este identificador de usuario está asignado de forma unívoca al usuario. En el momento de la compra del producto, un vendedor (no representado) transmite estos dos identificadores también a través de Internet 6 a la base de datos central 4. En la base de datos central 4 se almacena a continuación el "Tupel" (tuple o tuplo) formado por el identificador del usuario y el identificador del producto asignados uno a otro.

El usuario puede instalar en el ordenador 2 el programa que acaba de comprar. Durante la rutina de instalación se pide al usuario que conecte el dispositivo de almacenamiento USB 8 con el ordenador 2. La rutina de instalación lee del dispositivo de almacenamiento USB 8 el identificador del usuario y el identificador del producto y comprueba los mismos con ayuda de unos procedimientos adecuados. Esto puede realizarse, por ejemplo, mediante cifras de comprobación. Si el identificador del producto y el identificador del usuario coinciden con los valores requeridos, la rutina de instalación autoriza el proceso de instalación y el programa puede instalarse. Para la creación del identificador del usuario es posible que el mismo se genere en función del identificador del producto. Unos algoritmos pueden usar, por ejemplo, el identificador del producto para generar un identificador del usuario unívoco. De este modo puede comprobarse durante la instalación si el identificador de usuario almacenado en el dispositivo de almacenamiento USB 8 realmente se ha generado para el producto correspondiente o no.

Para el registro del producto, el ordenador 2 puede establecer a través de Internet 6 una conexión con la base de datos 4. Mediante esta conexión se transmite al menos el identificador del usuario y el identificador del producto a la base de datos central 4. En la base de datos central 4 se comprueba si estos dos valores están almacenados de forma asignada uno a otro. Si esto es el caso, la base de datos central 4 puede proceder al registro del producto. Además, puede procederse a otra autorización del producto instalado en el ordenador 2.

Según otra alternativa, en el dispositivo de almacenamiento USB 8 puede estar almacenado un identificador de producto y un identificador del hardware.

Cuando el usuario desea llamar, por ejemplo, mediante el ordenador 2 una oferta online a través de Internet 6 de un ordenador conectado con la base de datos central 4, al llamarse la página de Internet correspondiente se leen los identificadores de acceso del dispositivo de almacenamiento USB 8. Esto también puede realizarse de forma protegida por contraseña, de modo que los datos correspondientes sólo pueden leerse del dispositivo de almacenamiento USB mediante la entrada de una contraseña por parte del usuario.

Los identificadores leídos se transmiten a través de Internet 6 a la base de datos central 4. Allí se comprueba si los identificadores de acceso leídos están asignados uno a otro. Si esto es el caso, se autoriza nuevamente a través de Internet 6 el acceso a la página de Internet llamada.

También es posible que tras haber realizado una vez con éxito una llamada de la oferta online correspondiente, se modifique el primer identificador de acceso en el dispositivo de almacenamiento USB 8. Esto puede realizarse de tal modo que, tras haberse comprobado con éxito el "Tupel" (tuple o tuplo) de los identificadores de acceso en la base de datos 4, se calcule un primer identificador de acceso nuevo. Este primer identificador de acceso nuevo se almacena en la base de datos 4 junto con el segundo identificador de acceso anterior de forma asignada uno a otro. La asignación del primer identificador de acceso anterior al segundo identificador de acceso se anula.

A continuación, el primer identificador de acceso nuevo se transmite desde la base de datos 4 a través de Internet 6 al ordenador 2. Después de haberse recibido el primer identificador de acceso nuevo, éste se almacena en el dispositivo de almacenamiento USB 8. En el dispositivo de almacenamiento USB 8 están almacenados ahora el primer identificador de acceso nuevo y el segundo identificador de acceso. Al volver a llamar la oferta online, se transmite el primer identificador de acceso nuevo y el segundo identificador de acceso a la base de datos 4 realizándose allí con éxito una comparación.

En caso de haberse interceptado en la primera llamada el intercambio de datos entre el ordenador 2 y la base de datos 4 en Internet 6, habiéndose escuchado ilegalmente, por ejemplo, el primer identificador de acceso y el segundo identificador de acceso, mediante este mecanismo puede impedirse un nuevo acceso con el identificador de acceso anterior. De este modo existe una mayor seguridad para el usuario de la oferta online.

REIVINDICACIONES

1. Procedimiento para el control de una autorización de acceso a productos de software,

- en el que el producto de software es una oferta online que puede llamarse a través de una red de datos central,
- en el que un proveedor de los productos de software almacena al menos dos identificadores de acceso en un medio de almacenamiento intercambiable,
- en el que al menos un primer identificador de acceso es un identificador de producto asignado de forma unívoca al producto de software,
- en el que los identificadores de acceso se almacenan en una base de datos central de forma asignada uno a otro,
- en el que el segundo identificador de acceso puede ser modificado por un proveedor de tal modo
- que en el momento de una venta del producto de software se asigne un segundo identificador de acceso nuevo,
- que el segundo identificador de acceso nuevo se almacene junto con el identificador del producto en un medio de almacenamiento intercambiable,
- que el segundo identificador de acceso nuevo se asigne al identificador del producto en la base de datos central,
- en el que al menos los dos identificadores de acceso se leen del medio de almacenamiento intercambiable al accederse al producto de software,
- en el que se comprueba con ayuda de los dos identificadores de acceso leídos del medio de almacenamiento intercambiable una autorización de acceso de tal modo que los identificadores de acceso consultados se transmitan a través de la red de datos central a un ordenador o una red de ordenadores que gestionan la oferta online,
- que en el ordenador o en la red de ordenadores se compruebe si los identificadores de acceso se corresponden uno a otro,
- que se realice una autorización en caso de una comprobación positiva,
- que tras haberse accedido con éxito a la oferta online con ayuda del ordenador se modifique al menos el primer identificador de acceso y
- que la asignación entre al menos el primero y el segundo identificador de acceso se modifique correspondientemente en la base de datos central.

2. Procedimiento según la reivindicación 1, **caracterizado** porque los al menos dos identificadores de acceso se almacenan en una memoria USB o una tarjeta inteligente.

3. Procedimiento según la reivindicación 1, **caracterizado** porque al menos un segundo identificador de acceso es un identificador de hardware asignado de forma unívoca al medio de almacenamiento.

4. Procedimiento según la reivindicación 3, **caracterizado** porque la consulta de los identificadores de acceso del medio de almacenamiento está protegida por contraseña.

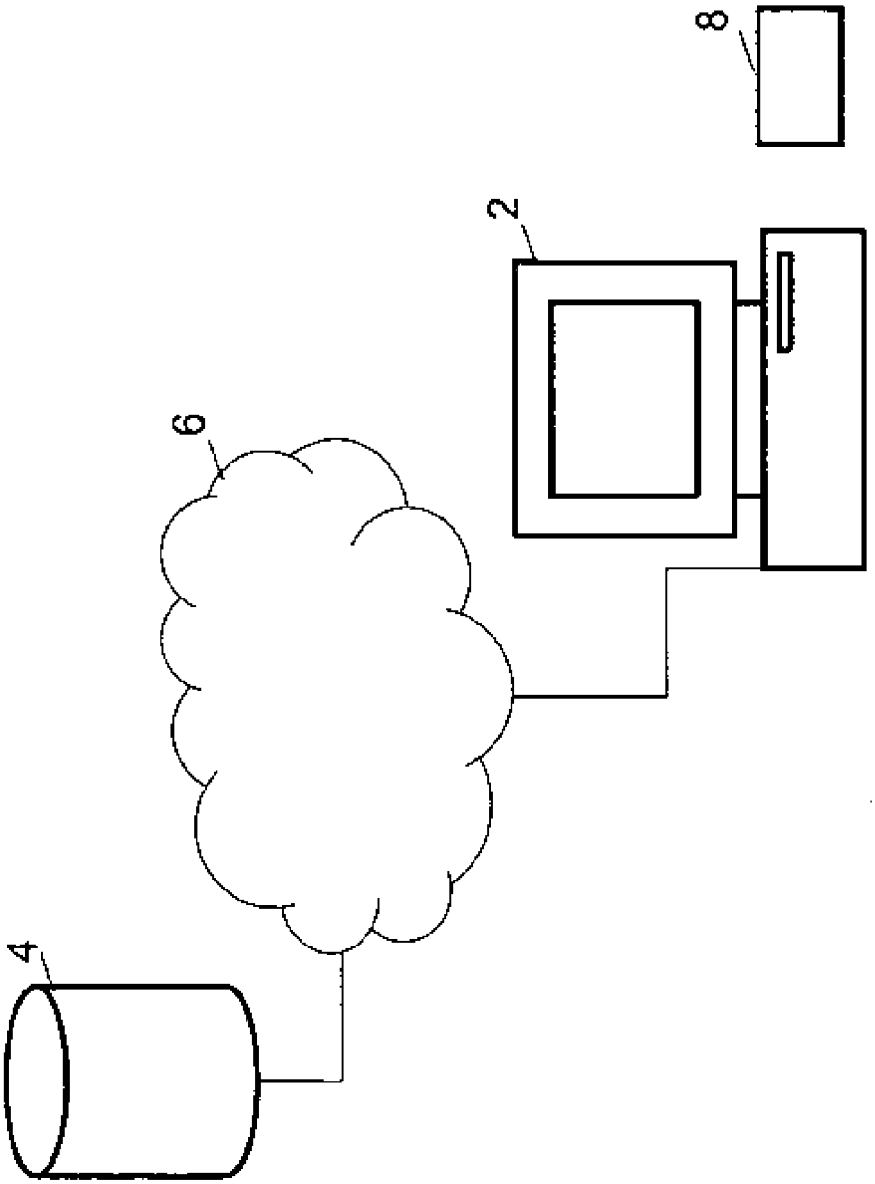

Fig. 1