



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 296 849**

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

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **02015065 .2**

86 Fecha de presentación : **18.10.1993**

87 Número de publicación de la solicitud: **1253504**

87 Fecha de publicación de la solicitud: **30.10.2002**

54 Título: **Procedimiento de utilización de programas informáticos y sistema informático para su aplicación.**

30 Prioridad: **23.10.1992 FR 92 12702**

73 Titular/es: **GEMPLUS**
avenue du Pic de Bertagne
Parc d'Activités de Gémenos
13420 Gémenos, FR

45 Fecha de publicación de la mención BOPI:
01.05.2008

72 Inventor/es: **Leroux, Jean-Yves**

45 Fecha de la publicación del folleto de la patente:
01.05.2008

74 Agente: **Cañadell Isern, Roberto**

ES 2 296 849 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 de utilización de programas informáticos y sistema informático para su aplicación.

La invención concierne un procedimiento de adquisición de programas informáticos por microordenadores.

La invención se refiere también a un sistema informático de adquisición de programas informáticos.

La invención se aplica, en particular, a los microordenadores dichos portátiles o de bolsillo, es decir, fácilmente transportables y pudiendo trabajar en alimentación autónoma (pilas, baterías).

Para obtener una autonomía de varias horas, fue necesario suprimir en estos microordenadores, los órganos muy consumidores. En particular, el disco duro fue sustituido por la memoria puramente electrónica, y los lectores de disquetes magnéticos fueron sustituidos por lectores de tarjetas de memoria de masa amovibles. Estas tarjetas de memoria se llaman PC-caras a veces en literatura anglosajona, o también tarjetas PCMCIA, del nombre de la norma correspondiente ("Personal Computer Memory Card International Association" 1030B East Duane Avenue, Sunnyvale, California). Estas tarjetas tienen varios chips de memoria y un conector en el extremo de la tarjeta (conector hembra de 68 husillos) enchufable en un conector correspondiente del lector del microordenador. Las conexiones son tales que la memoria puede enviarse por un puerto de entrada-salida paralelo al microordenador. Estas tarjetas tienen dimensiones reducidas: poseen el formato de una tarjeta de crédito con un grosor de 3 a 5 milímetros, y son de rápido acceso. Por fin, su capacidad de memoria total puede alcanzar varias decenas de megaoctetos.

Por otra parte, para proteger un ordenador contra una utilización por un usuario no habilitado, algunos microordenadores poseen igualmente un lector de tarjeta inteligente. La seguridad consiste en impedir la utilización del microordenador si el usuario no proporciona los códigos de confidencialidad adecuados, o si no introduce la tarjeta inteligente en este lector.

La distribución de programas informáticos aplicativos en los microordenadores se hace habitualmente por los disquetes magnéticos. En el supuesto de que estos microordenadores portátiles ya no tuvieran lectores de disquetes magnéticos, sino lectores de tarjetas PCMCIA, estos últimos se utilizan para garantizar la distribución de los programas informáticos aplicativos: un usuario compra a un vendedor una tarjeta PCMCIA en la que está cargado el programa informático aplicativo.

Pero en la práctica, las tarjetas PCMCIA a memoria de masa son muy caras, hasta varios miles de francos según la capacidad de memoria, lo que hace que el mínimo programa informático aplicativo sea carísimo.

La solicitud de Patente Europea 0 421 409 describe un sistema de transacciones asegurado en el que se comprueba cada mando con ayuda de una tarjeta inteligente.

La solicitud de Patente Europea 0 456 920 expone la gestión de la ejecución de un elemento remoto en un sistema distribuido de tratamiento de datos y derechos asociados a él.

Ya se conoce por la Patente US 4,941,175 un sistema de gestión de acceso conjunto a un mismo órgano informático. El documento referenciado US 4,941,175 permite bloquear el número de usuarios que tienen un acceso concomitante a un mismo órgano informático.

La presente invención tiene como objeto un nuevo procedimiento de adquisición de programas informáticos por microordenadores.

En la invención, se propone utilizar un servidor de base de datos en el que se almacenarán algunos programas informáticos aplicativos que deben distribuirse y un soporte de memoria electrónico amovible que contiene derechos de acceso a los programas informáticos para que sea posible descargar los programas informáticos aplicativos hacia un microordenador.

En efecto, la mayoría de los microordenadores contienen o pueden contener tarjetas que poseen funciones de comunicación entre el microordenador y el exterior. Estas tarjetas se llaman tarjetas con función Entrada/Salida. Un ejemplo típico: es el módem, que está conectado por un primer conector al microordenador y por un segundo conector a una línea telefónica para el envío o la recepción de datos digitales en la línea. En otro ejemplo de tarjeta con función de comunicación, la comunicación con el exterior se hace ya no por un conector a contactos materiales, sino por transmisión hertziana. Estas tarjetas pueden conectarse en un puerto de entrada/salida del microordenador o montarse directamente en el interior del microordenador.

Según la invención, se descargan programas informáticos aplicativos en un servidor de base de datos al que pueden conectarse microordenadores mediante esta tarjeta con función Entrada/salida. Se entregan (o se venden) a los usuarios soportes de memorización amovibles, que tienen muy poca memoria, estos soportes poseen un derecho de acceso a por lo menos un programa informático aplicativo. En este caso, este tipo de soporte que no tiene prácticamente memoria tiene un coste bajo, unos veinte francos como máximo. Las informaciones almacenadas sólo utilizan algunos octetos. El soporte puede ser por ejemplo una tarjeta inteligente del tipo tarjeta de crédito, e incluso una

tarjeta PCMCIA con una memoria muy reducida, el microordenador comprende los lectores correspondientes a estas tarjetas.

Cuando un usuario de un microordenador desea adquirir un programa informático aplicativo, compra entonces el soporte que incluye el derecho de acceso a este programa informático. El precio del soporte comprado corresponderá al precio de venta del programa informático añadido al del soporte, el cual sólo cuesta unos veinte francos aproximadamente. Seguidamente, el usuario introduce el soporte en el lector del microordenador.

Se conecta al servidor y selecciona, por ejemplo, a través de la pantalla y del teclado del microordenador, el programa informático aplicativo deseado. El servidor controlará entonces el derecho de acceso al soporte, vía el microordenador, luego transferirá el programa informático aplicativo hacia el microordenador, por ejemplo a su memoria interna.

De manera más precisa, el procedimiento de adquisición de programas informáticos según la invención se caracteriza principalmente por las siguientes etapas:

- en una primera etapa, se descargan algunos programas informáticos en un servidor de base de datos al cual pueden estar conectados microordenadores en condiciones de recibir soportes de memorización amovibles, y entregar a los usuarios de los microordenadores soportes de memorización amovibles que contienen por lo menos un derecho de acceso a un programa informático del servidor,
- en una segunda etapa, el usuario de un microordenador introduce el soporte de memorización que posee y un programa informático deseado del servidor y autorizado por el soporte se descarga hacia el microordenador.

En un ejemplo, el programa informático se descarga en memoria interna. También puede descargarse en una tarjeta PCMCIA, cuando los microordenadores disponen de un número de lectores suficiente.

El tiempo de descarga del programa informático sólo depende del tamaño del programa informático y de las características de transmisión (formato, velocidad) de la conexión microordenador/servidor (conexión módem, red inalámbrica, etc).

Según otra característica de la invención, el servidor controla el derecho de acceso utilizando procedimientos de seguridad con identificación y algoritmos de codificación/descifrado. El soporte de memorización comprende con este fin un módulo electrónico de seguridad que lo hace inviolable. En efecto, es necesario impedir a los defraudadores piratear las informaciones contenidas en los soportes, lo que permitiría descargar programas informáticos sin haber pagado el precio, realizando soportes fraudulentos.

Por módulo electrónico de seguridad, se entiende aquí un chip de circuito integrado que incluye una memoria no volátil con informaciones confidenciales, y un circuito de seguridad programado, en condiciones de utilizar estas informaciones confidenciales y otras informaciones proporcionadas por el usuario, para entregar instrucciones de validación, después de comprobar una relación predeterminada entre estos dos tipos de información. Los datos confidenciales no salen del módulo de seguridad.

Según otro aspecto de la invención, se asegura la propia utilización de los programas informáticos aplicativos.

El procedimiento se caracteriza entonces principalmente del siguiente modo:

- se entrega a un usuario un soporte de memorización amovible que contiene derechos de utilización, propios por lo menos a un programa informático del servidor y autorizando la descarga del o de los programas informáticos correspondientes;
- entonces el usuario debe introducir el soporte de memorización que contiene los derechos de utilización propios al programa informático que desea descargar y mandar ejecutar. En efecto, el programa informático descargado está ventajosamente auto-asegurado, su ejecución incluye accesos al soporte de memorización para controlar los derechos de utilización secretos y autorizar o no el resto de la ejecución.

Otras particularidades y ventajas de la invención se pondrán de manifiesto cuando se lea la descripción que se hace a título indicativo y no limitativo de la invención y en referencia al dibujo anexo en el cual:

- la figura 1 representa un esquema de un sistema informático según la invención,

Un sistema informático conforme a la invención está representado en la figura 1. Éste incluye un servidor de base de datos 1, en el que se almacenan algunos programas informáticos aplicativos 10, un microordenador 2 conectado al servidor por una interfaz 3 - red telefónica, radiotelefónica u otros - y un soporte de memorización electrónico amovible 4.

ES 2 296 849 T3

El microordenador incluye: una pantalla 20, un teclado 21, que puede ser sustituido por un lápiz o cualquier otra interfaz hombre-máquina existente, una unidad central 22, una memoria interna 23 y un lector 24 de soporte de memorización electrónico amovible.

5 El soporte de memorización incluye una interfaz 40 de conexión al lector 24 del microordenador; un microprocesador de memoria no volátil 41. El soporte de memorización contiene en memoria 41 informaciones secretas que corresponden a un derecho de acceso a uno o varios programas informáticos aplicativos almacenados en el servidor 1. En la práctica, estos soportes los vende el vendedor distribuidor de programas informáticos aplicativos en cuestión.

10 Para proceder a la adquisición de un programa informático aplicativo, el usuario que posee un soporte que contiene el derecho de acceso correspondiente, debe introducirlo en el lector 24 del microordenador. Seguidamente, el usuario lanza en el microordenador un programa informático de conexión al servidor. Cuando se establece la comunicación con el servidor, este último visualiza en la pantalla del microordenador un menú gracias al cual el usuario elige el(los) programa(s) informático(s) aplicativo(s) que desea adquirir. El servidor controlará entonces el derecho de acceso a
15 estos programas informáticos interrogando al soporte vía la unidad central del microordenador. Este control se efectúa ventajosamente utilizando procedimientos de seguridad similares a aquellos utilizados en las tarjetas inteligentes (tarjetas de crédito), es decir, con procedimiento de identificación, autenticación, utilizando algoritmos de codificación, decodificación. Las informaciones secretas no se transmiten al exterior del soporte. El chip electrónico de memoria no volátil 41 posee entonces un conjunto de circuitos de seguridad programado para garantizar estas funciones de
20 seguridad.

Si el control de seguridad es positivo, el servidor efectúa la descarga del(o de los) programa(s) informático(s) aplicativo(s) seleccionado(s) y autorizados) por el soporte, en la memoria interna del microordenador. En opción, puede preverse, para un microordenador que tiene al menos dos lectores de soportes de memorización electrónica 24 y
25 25 amovibles, que el usuario pueda elegir dónde el lugar donde debe descargarse el programa informático: en memoria interna 23 del microordenador o en un soporte amovible 5 que incluye un microprocesador 50 de memoria viva, por ejemplo. El programa informático descargado puede entonces ejecutarlo el microordenador.

Ahora bien, podemos imaginar que en el momento de la descarga, un defraudador haya podido memorizar el
30 programa informático. Preferiblemente, se elegirá un procedimiento de descarga codificado. Pero ventajosamente, para asegurar el procedimiento de la invención, está previsto un soporte de memorización electrónico amovible que debe introducirse en el lector en el momento de la ejecución del programa informático aplicativo y que contiene datos secretos que corresponden a derechos de utilización conocidos por el programa informático. Este último, durante su ejecución, interroga de vez en cuando al soporte de memorización con el fin de controlar que existen debidamente los
35 derechos de utilización. Este control se hará, preferiblemente, utilizando los procedimientos de seguridad conocidos y, en particular, los algoritmos de codificación-decodificación. El soporte de memorización contiene un chip de seguridad para este fin.

Ventajosamente, el mismo soporte de memorización 4 contiene los derechos de acceso a un programa informático
40 aplicativo y los derechos de utilización correspondientes en el mismo chip electrónico 41.

Pueden preverse otras opciones. Por ejemplo, está previsto que el programa informático aplicativo se venda para un número limitado de utilizaciones. El chip electrónico incluirá entonces, por ejemplo, un contador que contiene esta información. Una tarea del programa informático aplicativo incluirá por ejemplo las siguientes etapas:

- 45
- ir a leer en el soporte de memorización amovible 4, una información que indicará si el programa informático fue adquirido para un número limitado de utilizaciones. En caso contrario, esta tarea se termina y la ejecución continua;
 - 50 - en caso afirmativo, enviar un orden de decrementación. El chip electrónico controla en interno el contenido del contador y si no es nulo, expide una validación hacia los microordenadores. El programa informático puede seguir la ejecución;
 - 55 - pero si el contador es nulo, envía un mensaje de error por ejemplo, y el programa informático interrumpe su ejecución.

En un ejemplo de aplicación práctico, el soporte memoria amovible 4 es una tarjeta inteligente, o una tarjeta que sólo contiene el chip electrónico necesario para la aplicación. El microordenador estará equipado de lectores correspondientes para leer estas tarjetas. El chip electrónico 41, contiene, por ejemplo, un conjunto de circuitos 410
60 de seguridad programada, un conjunto de circuitos 411 de memoria no volátil y un contador 412.

El conjunto de circuitos 410 de seguridad controla el acceso a la memoria y al contador, y ventila los accesos externos del soporte.

65

REIVINDICACIONES

1. Procedimiento asegurado de utilización de un programa informático (10) en un microordenador (2) que consiste en introducir un soporte de memorización electrónico amovible (4) que contiene datos secretos que corresponden a los derechos de utilización del programa informático en el microordenador (2), **caracterizado** porque consiste en realizar el programa informático (10) interrogando de vez en cuando el soporte de memorización (4) con el fin de controlar los derechos de utilización.

2. Procedimiento asegurado de utilización de un programa informático (10) según la reivindicación 1, **caracterizado** porque el soporte de memorización electrónico amovible (4) contiene por otro lado los derechos de acceso al programa informático (10) con el fin de descargarlo desde un servidor (1) antes de su utilización.

3. Procedimiento asegurado de utilización de un programa informático (10) según una de las reivindicaciones anteriores, **caracterizado** porque el soporte de memorización amovible (4) posee un contador que indica un número limitado de utilizaciones autorizadas, este contador está decrementado a la ejecución del programa informático (10), el soporte (4) verifica el estado del contador para autorizar o no la ejecución del programa informático (10).

4. Soporte amovible de memorización electrónica (4) **caracterizado** porque incluye datos secretos que corresponden a derechos de utilización de un programa informático (10) y porque está en condiciones de autorizar o no la ejecución de un programa informático (10) en un microordenador (2) en función de estos derechos interrogando de vez en cuando al soporte de memorización (4) con el fin de controlar los derechos de utilización.

5. Soporte amovible de memorización electrónica (4) según la reivindicación 4 **caracterizado** porque posee por otro lado derechos de acceso a un programa informático (10) con el fin de autorizar o no su descarga desde un servidor (1) en un microordenador (2).

6. Soporte amovible de memorización electrónica (4) según una de las reivindicaciones 4 ó 5, **caracterizado** porque contiene un medio para limitar el número de utilizaciones de un programa informático (10) en un microordenador (2).

7. Soporte amovible de memorización electrónica (4) según una de las reivindicaciones 4 a 6 **caracterizado** porque es una tarjeta inteligente.

8. Soporte amovible de memorización electrónica (4) según una de las reivindicaciones 4 a 6 **caracterizado** porque es una tarjeta PCMCIA.

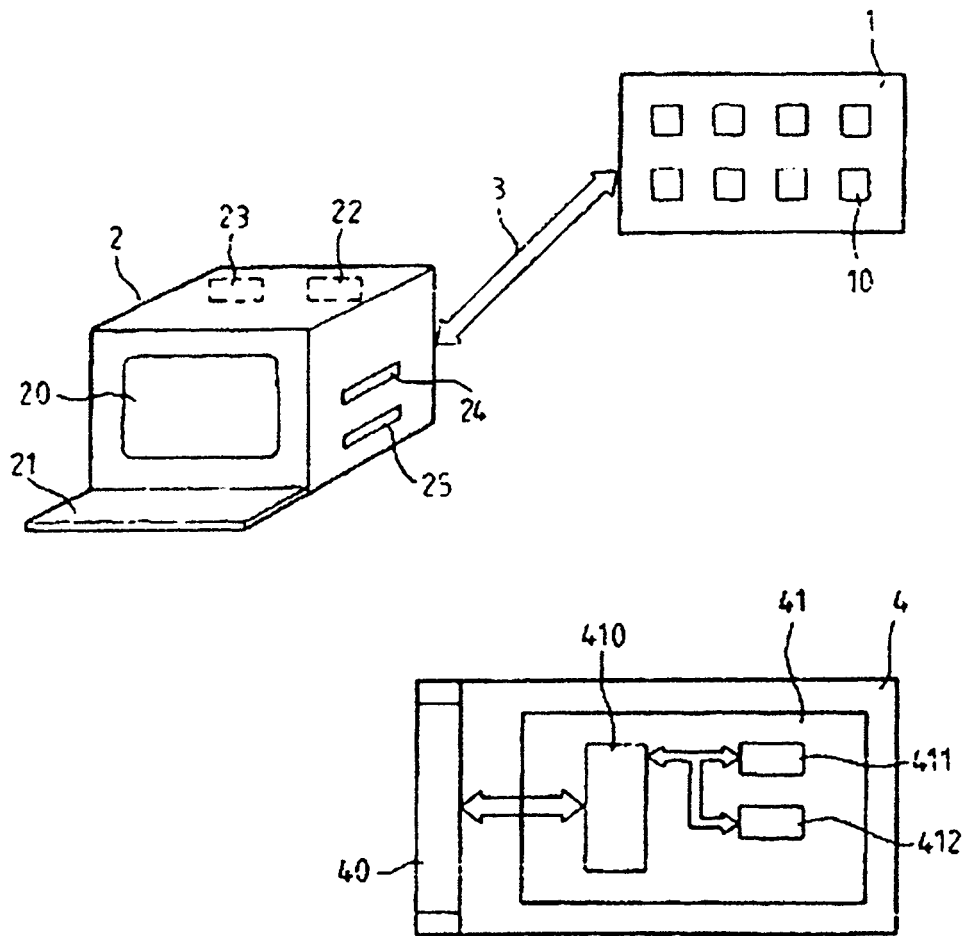


FIG. 1