(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 626 147**

(51) Int. CI.:

***G06F 21/83*** (2013.01)
***G06F 21/44*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.12.2011 PCT/FR2011/053197**

(87) Fecha y número de publicación internacional: **05.07.2012 WO12089983**

(96) Fecha de presentación y número de la solicitud europea: **26.12.2011 E 11815546 (4)**

(97) Fecha y número de publicación de la concesión europea: **15.03.2017 EP 2659419**

(54) Título: **Procedimiento y dispositivo de control de acceso a un sistema informático**

(30) Prioridad:

**27.12.2010 FR 1061285**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**24.07.2017**

(73) Titular/es:

**ELECTRICITÉ DE FRANCE (50.0%)**
**22-30 Avenue de Wagram**
**75008 Paris, FR y**
**SECLAB (50.0%)**

(72) Inventor/es:

**SITBON, PASCAL;**
**TARRAGO, ARNAUD y**
**NGUYEN, PIERRE**

(74) Agente/Representante:

**VEIGA SERRANO, Mikel**

## DESCRIPCIÓN

Procedimiento y dispositivo de control de acceso a un sistema informático

**Sector de la técnica**

La invención se refiere al campo del acceso seguro a unos sistemas informáticos y, en concreto, al del control del acceso a estos sistemas informáticos por medio de periféricos particulares.

**Estado de la técnica**

Los sistemas informáticos existentes presentan un cierto número de puertos que permiten la conexión de diferentes tipos de periféricos que sirven tanto para la interfaz con los usuarios, para la conexión hacia otros sistemas informáticos como para el almacenamiento de datos.

De este modo, estos sistemas informáticos pueden sufrir en su integridad por el empalme físico de ciertos periféricos que alojan unos datos maliciosos, incluido sin el conocimiento del usuario sobre los puertos de estos sistemas.

Este puede ser, en concreto, el caso con los periféricos USB (para Universal Serial Bus en inglés). De hecho, los puertos USB son unos puertos universales de tipo "multifunciones" en el sentido en que pueden aceptar toda una gama de periféricos de tipos diferentes, como, por ejemplo, unas interfaces de red, unos elementos de almacenamiento de tipo llave USB, unos teclados, unos ratones, unas cámaras web, etc.

Este carácter universal de estos puertos, ventajoso desde el punto de vista de la flexibilidad en cuanto a empalme y a funciones soportadas ofrecida por una interfaz de este tipo, resulta problemático en un entorno en que la seguridad se convierte en un factor esencial, pues permite la conexión de periféricos que alojan unos datos maliciosos sobre los puertos USB de sistemas informáticos sensibles cuyo acceso debería estar protegido.

Un usuario malicioso (resp. negligente), que utiliza un periférico de este tipo que aloja, por ejemplo, unos datos no deseables, puede tomar, de este modo (resp. perder) el control, instalar unos virus o grabar unos datos confidenciales de un sistema informático sensible, gracias a la sola presencia de puertos USB sobre este sistema a los que puede conectar tal tipo de periféricos.

No es posible desterrar mera y sencillamente la utilización de estos puertos universales en la medida en que estos puertos son necesarios para la utilización de ciertos periféricos esenciales, como, por ejemplo, los ratones o los teclados.

Para responder a este problema, se han propuesto unas soluciones de software en las que ciertos tipos de periféricos tienen acceso a ciertas funciones, gestionándose el acceso a las funciones en forma meramente de software. De este modo, la solicitud de los Estados Unidos US 2006/0037084 divulga un sistema de control de acceso de diferentes puertos USB a un cierto número de funcionalidades, seleccionadas y configurables dinámicamente por medio de un sistema de explotación que utiliza unas informaciones memorizadas de configuración.

El documento KR 2007 0017609 A divulga un dispositivo de control de acceso interpuesto entre el puerto USB de un sistema informático y un periférico USB. Un controlador de seguridad permite el acceso al sistema informático obteniendo los identificadores del fabricante, del producto y de la clase de interfaz (categoría) del periférico y comparándolos con una lista de objetos permitidos y/o prohibidos almacenada de forma permanente en una memoria flash. Dicha memoria solo puede modificarse por un gestor de seguridad.

Estas soluciones de software presentan, sin embargo, la desventaja de que son complejas de gestionar y eludibles mediante unas vulnerabilidades relacionadas con el sistema de explotación empleado y de la manera en que gestiona estos periféricos o de la manera en que se administra el sistema informático. El usuario de un periférico que aloja unos datos maliciosos, tomando el control de un sistema de explotación de este tipo, puede reconfigurar entonces las funciones accesibles en los puertos USB y acceder al sistema informático con este periférico o difundir entonces el contenido malicioso sobre el sistema informático o por medio de los derechos de administración de este sistema.

**Objeto de la invención**

La presente invención tiene como objeto remediar los inconvenientes anteriormente citados.

Tiene como objeto proponer un control de acceso a unos sistemas informáticos, por mediación de puertos universales, que no pueda usarse indebidamente por medio de un usuario malicioso o negligente y que sea sencillo de gestionar.

Propone para ello un dispositivo de control de acceso a un sistema informático, comprendiendo el dispositivo al menos un puerto multifunciones adecuado para conectarse a diferentes categorías de periféricos y una interfaz de acceso adecuada para conectarse al sistema informático, estando el dispositivo caracterizado por que comprende unos medios de gestión de acceso conectados entre el puerto multifunciones y la interfaz, estando los medios de gestión de acceso configurados físicamente para permitir el acceso de la interfaz por medio de un periférico conectado al puerto multifunciones solamente si dicho periférico pertenece a una categoría de periféricos asociada específicamente y de forma permanente al puerto multifunciones al que está conectado.

Según un modo de realización en que este dispositivo comprende un primer y un segundo puertos multifunciones, los medios de gestión de acceso están configurados físicamente para permitir el acceso de la interfaz por medio de un periférico conectado al primer puerto multifunciones solamente si este periférico pertenece a una primera categoría de periféricos asociada específicamente y de forma permanente al primer puerto multifunciones y para permitir el acceso de la interfaz por medio de un periférico conectado al segundo puerto multifunciones solamente si este periférico pertenece a una segunda categoría de periféricos asociada específicamente y de forma permanente al segundo puerto multifunciones y distinta de la primera categoría de periféricos.

Según un modo de realización en que comprende, además, un tercer puerto multifunciones, los medios de gestión de acceso están configurados físicamente para permitir el acceso de la interfaz por medio de un periférico conectado al tercer puerto multifunciones solamente si este periférico pertenece a una tercera categoría de periféricos asociada específicamente y de forma permanente al tercer puerto multifunciones y distinta de las primera y segunda categorías de periféricos.

En un modo particular de realización, los medios de gestión de acceso comprenden un primer módulo de acceso, un segundo módulo de acceso y un tercer módulo de acceso conectados respectivamente al primer puerto multifunciones, al segundo puerto multifunciones y al tercer puerto multifunciones y la interfaz de acceso comprende un módulo hub conectado a dichos primero, segundo y tercer módulo de acceso.

Ventajosamente, los medios de gestión de acceso comprenden un módulo de identificación configurado para identificar la categoría de dicho periférico y para conectar la interfaz al puerto multifunciones al que está conectado el periférico solamente si la categoría identificada del periférico corresponde a la categoría de periféricos asociada específicamente y de forma permanente a dicho puerto multifunciones.

Según un modo de realización, los medios de gestión de acceso comprenden unos medios de memorización con el fin de memorizar la categoría de periféricos asociada específicamente y de forma permanente a dicho puerto multifunciones. Por ejemplo, los medios de memorización pueden ser de tipo memoria de solo lectura. De esta manera, la asociación entre un puerto multifunciones y una categoría de periféricos (memorizada en la memoria de solo lectura) para los que está permitido el acceso, es ventajosamente permanente.

En una realización, los medios de gestión de acceso son unos circuitos programables una sola vez tales como, por ejemplo, unos circuitos de tipo FPGA (para "Field-Programmable Gate Array"), circuitos programables que están configurados para no modificarse ya después de su programación. De este modo, ventajosamente, los circuitos programables ya no son modificables por unos terceros u otros programas maliciosos.

En un modo de realización ventajoso, los medios de gestión de acceso comprenden, además, un módulo de verificación, conectado entre los medios de gestión de acceso y la interfaz, configurado para efectuar una verificación sobre los datos transmitidos entre el puerto multifunciones y la interfaz.

En particular, la primera, la segunda y/o la tercera categoría de periféricos corresponden a una categoría de periféricos de entre los teclados, los ratones y las llaves de almacenamiento.

En un modo particular de realización, el puerto multifunciones es un puerto universal de tipo USB.

La invención propone, además, un procedimiento de control de acceso de un periférico a un sistema informático por medio de un dispositivo de control de acceso que comprende un puerto multifunciones al que está conectado el periférico y una interfaz a la que está conectado el sistema informático, comprendiendo este procedimiento el permiso de acceso, para el periférico, a la interfaz conectada al sistema informático solamente si dicho periférico pertenece a una categoría de periféricos asociada específicamente y de forma permanente al puerto multifunciones al que está conectado dicho periférico.

Ventajosamente, este procedimiento comprende una etapa de identificación de la categoría de dicho periférico por el dispositivo, permitiéndose el acceso a la interfaz solamente si la categoría identificada del periférico corresponde a la categoría de periféricos específicamente asociada al puerto multifunciones al que está conectado el periférico.

De forma ventajosa, este procedimiento comprende una etapa de verificación de los datos transmitidos, después del permito de acceso, entre el puerto multifunciones al que está conectado el periférico y la interfaz del dispositivo conectada al sistema informático.

Según un modo de realización ventajoso, el procedimiento comprende una etapa previa de asociación física permanente de una categoría específica de periféricos respectivamente a cada uno de dichos al menos un puerto multifunciones del dispositivo, siendo estas categorías específicas de periféricos distintas las unas de las otras.

La presente invención propone igualmente un programa de ordenador que incluye unas instrucciones de código para la implementación del procedimiento de control de acceso de anteriormente, cuando este programa se ejecuta por el procesador de un dispositivo de control de acceso que conecta un periférico a un sistema informático. Un programa de este tipo debe considerarse como un producto en el marco de la protección que se busca por la presente solicitud de patente.

**Descripción de las figuras**

Otras características y ventajas de la invención se mostrarán con el examen de la descripción detallada de a continuación y de los dibujos adjuntos en los que:

- la figura 1 es un esquema sinóptico que ilustra un dispositivo de control de acceso según la presente invención;
- las figuras 2A a 2C ilustran tres modos de realización particulares del dispositivo de control de acceso de la figura 1; y
- la figura 3 ilustra las etapas de un procedimiento de acceso controlado a un sistema informático según la presente invención.

**Descripción detallada de la invención**

Se hace referencia en primer lugar a la **figura 1** en la que se ilustra un dispositivo de control de acceso según la presente invención.

Este dispositivo de control de acceso DISP comprende un cierto número de puertos multifunciones $U_1$, $U_2$, $U_3$,..., $U_i$, que permiten la conexión de un periférico P.

Un solo y único puerto multifunción $U_1$ puede emplearse en este dispositivo DISP, pero la invención es más particularmente ventajosa cuando se emplean una pluralidad de puertos multifunciones, como se explicará esto a continuación.

Se designa en este caso por la expresión de "puerto multifunciones" cualquier puerto universal que permite la conexión de periféricos que pertenecen a diferentes categorías de periféricos, por oposición a un "puerto monofunción" dedicado a un solo y único tipo de periférico, como es este el caso, por ejemplo, con los puertos PS/2 (uso limitado a la conexión de periféricos usuarios de tipo ratón o teclado), los puertos IEEE 1394 o los puertos Ethernet (uso limitado a la conexión de equipos de red), los puertos VGA (uso limitado a la conexión de pantallas), etc...

A título de ejemplo, se pueden citar en este caso los puertos USB como puerto multifunciones, en la medida en que unos puertos USB de este tipo pueden permitir la conexión de periféricos que pertenecen a unas categorías tan diversas como los ratones, los teclados, las unidades de almacenamiento, los módems, las interfaces de redes, las cámaras web, etc.

El dispositivo de control de acceso DISP comprende igualmente una interfaz de acceso INT que permite la conexión del dispositivo DISP a un sistema informático.

Se entiende en este caso por la expresión de "sistema informático" cualquier sistema o dispositivo capaz de tratar informáticamente unos datos, ya sea un ordenador personal PC, un servidor SERV o una placa base PB, como se ilustra.

En los dos primeros casos, el dispositivo DISP puede tomar la forma de una carcasa externa que puede conectarse entre el periférico P y el ordenador PC o el servidor SERV, por medio de una interfaz tradicional. En el último caso, la interfaz INT puede ser de tipo PCI y el dispositivo DISP puede tomar la forma de una tarjeta interna que puede conectarse a una placa base PB situada en el interior de una carcasa de ordenador.

El dispositivo DISP comprende, además, unos medios de gestión de acceso $M_{acc}$, conectados entre los puertos multifunciones $U_1$, $U_2$, $U_3$,..., $U_i$, por mediación de un controlador CONT y la interfaz de acceso INT. Estos medios de gestión de acceso $M_{acc}$ están configurados físicamente para permitir el acceso de la interfaz de acceso INT por medio del periférico P, cuando este periférico P está conectado al puerto multifunciones $U_i$, solamente si este periférico P pertenece a una categoría de periféricos asociada específicamente y de forma permanente al puerto multifunciones.

Para ello, los medios de gestión de acceso $M_{acc}$ asocian respectivamente a cada uno de los puertos multifunciones

$U_1$, $U_2$, $U_3$,..., $U_i$ una sola y única categoría $CP_i$ de periféricos. Esta asociación, específica para cada puerto multifunciones, se efectúa de manera permanente y no modificable, de forma física, durante el diseño físico de los medios de gestión de acceso, con el fin de impedir que un usuario malicioso modifique esta asociación específica.

De este modo, a cada puerto multifunciones $U_1$, $U_2$, $U_3$,..., $U_i$ está asociada una sola y única categoría $CP_i$ de periféricos. Una categoría de este tipo $CP_i$ de periféricos puede elegirse de entre las categorías distintas siguientes, cuya lista de más abajo no es exhaustiva:

- teclados de ordenadores;
- ratones de ordenadores;
- periféricos de almacenamiento USB;
- impresoras;
- lector de tarjeta de chip;
- periféricos de audio;
- periféricos de imagen;
- periféricos de vídeo;

Una asociación de este tipo permanente de categoría de periféricos específicos a cada puerto multifunciones $U_1$, $U_2$, $U_3$,..., $U_i$, puede efectuarse realizando los medios de gestión de acceso $M_{acc}$ en forma de un circuito programable, por ejemplo, de tipo FPGA, que no puede modificarse ya después de programación de este circuito y que evita tener que recurrir a un software para controlar el acceso a la interfaz INT. De este modo, sea el que sea el nivel de seguridad del sistema informático al que el dispositivo DISP sirve de intermediario para la conexión de un periférico P, este dispositivo DISP asegura un nivel de seguridad autónomo y preventivo.

Estos medios de gestión de acceso $M_{acc}$ pueden presentarse en forma de un único módulo que gestiona el acceso de todos los puertos multifunciones a la interfaz INT o bien en forma de varios módulos dedicados a la gestión de acceso específico de algunos de los puertos multifunciones a la interfaz INT, por ejemplo, un módulo dedicado a la gestión del acceso de periféricos de almacenamiento a la interfaz INT y un módulo dedicado a la gestión del acceso de periféricos de tipo ratón o teclado a la interfaz INT.

De este modo, en un modo de realización en que el dispositivo DISP comprende un primer puerto multifunciones $U_1$ y un segundo puerto multifunciones $U_2$, sus medios de gestión de acceso $M_{acc}$ están configurados físicamente para permitir el acceso de la interfaz INT por medio del periférico P, cuando está conectado al primer puerto multifunciones $U_1$, solamente si este periférico P pertenece a una primera categoría $CP_1$ de periféricos asociada específicamente y de forma permanente al primer puerto multifunciones $U_1$.

En este modo de realización, los medios de gestión de acceso $M_{acc}$ del dispositivo DISP están configurados, además, para permitir el acceso de la interfaz INT por medio del periférico P, cuando está conectado al segundo puerto multifunciones $U_2$, solamente si este periférico P pertenece a una segunda categoría $CP_2$ de periféricos asociada específicamente y de forma permanente al segundo puerto multifunciones $U_2$ y distinta de la primera categoría $CP_1$ de periféricos.

En otro modo de realización en que, además de los primero y segundo puertos multifunciones $U_1$ y $U_2$, asociados respectivamente a las categorías $CP_1$ y $CP_2$ de periféricos, el dispositivo DISP comprende un tercer puerto multifunciones $U_3$, los medios de gestión de acceso $M_{acc}$ están configurados físicamente para permitir el acceso de la interfaz INT por medio del periférico P, cuando está conectado al tercer puerto multifunciones $U_3$, solamente si este periférico P pertenece a una tercera categoría $CP_3$ de periféricos asociada específicamente y de forma permanente al tercer puerto multifunciones $U_3$ y distinta de las primera y segunda categorías de periféricos $CP_1$ y $CP_2$.

En un modo de realización ventajoso, los medios de gestión de acceso $M_{acc}$ comprenden un módulo de identificación $M_{id}$.

Este módulo de identificación $M_{id}$ está configurado, por una parte, para identificar la categoría CP de periférico a la que pertenece el periférico P cuando se conecta al puerto multifunciones $U_i$.

De este modo, en el caso ilustrativo de puertos multifunciones de tipo USB, se transmite un dato de identificación de la categoría de periférico sobre un controlador USB, en forma de dos números hexadecimales, durante la conexión del periférico a un puerto USB.

Un dato de este tipo de identificación se encuentra, en concreto, definido en el campo "bDeviceClass", dicho de otra manera, en forma de un código de clase predefinido en la norma USB, presente en los "descriptores de aparatos" igualmente definidos según la norma USB.

Sin embargo, como la identificación de un periférico no siempre se efectúa sistemáticamente con un campo estático, es igualmente posible observar varios intercambios entre el periférico P y el sistema informático central PC o SERV, antes de determinar la categoría CP del periférico P. Al estar el dispositivo DISP situado físicamente entre el

periférico P y el sistema informático central, este dispositivo dispone de toda la latitud para determinar con precisión la categoría CP del periférico P. Este dispositivo puede, según la categoría y los intercambios observados, decidir hacer pasar los intercambios sin modificarlos, filtrarlos y/o modificar (por ejemplo, restricción de los controles, de los datos sobre el tamaño, el contenido, etc.) o hacer no operativo el periférico. En este último caso, el periférico se verá como desconectado por el sistema informático central.

A título de ejemplo, los campos "bDeviceClass" siguientes, utilizados en la norma USB, se indican a título meramente ilustrativo en la tabla 1 de más abajo:

**Tabla 1: lista de las categorías de periféricos asociadas a unos códigos de clase "bDeviceClass" predefinido en la norma USB**

| Valor del campo "bDeviceClass" | Tipo de periférico designado por el código de clase |
|---|---|
| 00 | Cada interfaz precisa su propio código de clase |
| 01 | Periférico de audio |
| 02 | Periférico de control y de comunicaciones |
| 03 | Interfaz hombre-máquina (HID) |
| 05 | Periférico físico |
| 06 | Periférico de imagen |
| 07 | Periférico de impresión |
| 08 | Periférico de almacenamiento masivo |
| 09 | Hub |
| 0E | Periférico de vídeo |
| E0 | Controlador inalámbrico |
| FF | Código de clase precisado por el vendedor |

De este modo, en el caso en que los puertos multifunciones son unos puertos universales de tipo USB y en que el controlador CONT es un controlador USB, el módulo de identificación $M_{id}$ puede identificar la categoría CP de un periférico P conectado al puerto multifunciones $U_i$ interceptando los datos denominados de "descripción de aparato" intercambiados sobre el controlador USB durante la conexión de este periférico P.

El módulo de identificación $M_{id}$ puede entonces, mediante la extracción de estos datos de "descripción de aparato" (código de clase del periférico P indicado en el campo "bDeviceClass" y otros campos como el subClass y el interfaceClass, etc.) y mediante la observación de los intercambios entre el periférico P y la interfaz INT, deducir de ello de este código de clase la categoría CP de este periférico P.

Este módulo de identificación $M_{id}$ está, por otra parte, configurado para conectar la interfaz INT a este puerto multifunciones $U_i$ solamente si la categoría CP identificada del periférico corresponde a la categoría de periféricos $CP_i$ asociada específicamente y de forma permanente a este puerto multifunciones $U_i$.

La transferencia de datos entre el periférico P y un sistema informático conectado a la interfaz INT solo podrá tener lugar entonces si el periférico P es ciertamente del tipo previsto específicamente para conectarse al puerto multifunciones $U_i$.

Se puede considerar igualmente modificar el tipo de periférico sobre la marcha, con el fin de ocultar la verdadera naturaleza al sistema informático central.

Por ejemplo, cuando el usuario conecta un teclado "multifunciones" con unas teclas programables al dispositivo DISP, este dispositivo DISP puede anunciar solo al sistema informático un teclado normal 105 teclas, el cual recurre al piloto por defecto del sistema informático. En este caso, solo las teclas tradicionales del teclado "multifunciones" estarán visibles por el sistema informático.

Además de esta restricción del tipo, el dispositivo DISP puede validar entonces, modificar o suprimir, sobre la marcha ciertas acciones durante unos intercambios entre el periférico y sistema informático central. Por ejemplo, es posible prohibir (físicamente) cualquier solicitud de escritura hacia un periférico de almacenamiento.

Con el fin de implementar estas dos funcionalidades de identificación y de conexión, el módulo de identificación $M_{id}$ puede aplicarse físicamente en forma de un procesador PROC conectado, por una parte, al controlador CONT, con

el fin de recibir unos datos emitidos durante la conexión del periférico P a puerto multifunciones $U_i$ y, por otra parte, a unos medios de memorización MEM de tipo memoria de solo lectura en el que están memorizadas de forma permanente, para cada puerto multifunciones $U_1$,..., $U_i$ del dispositivo DISP, la categoría de periféricos $CP_1$,..., $CP_i$ específicamente asociada respectivamente al puerto multifunciones $U_1$,..., $U_i$.

El procesador PROC del módulo de identificación $M_{id}$ utiliza entonces los datos recibidos del controlador CONT para encontrar en los medios de memorización MEM la categoría de periféricos $CP_i$ específicamente asociada al puerto multifunciones $U_i$, verifica si la categoría CP identificada del periférico P corresponde ciertamente a esta categoría $CP_i$ y permite la conexión (es decir, la transferencia de datos entre el periférico P y la interfaz INT si el resultado de esta verificación es positivo.

En un modo de realización ventajoso, los medios de gestión de acceso $M_{acc}$ comprenden, además, un módulo de verificación $M_{VERIF}$, conectado entre los medios de gestión de acceso $M_{acc}$ y la interfaz INT y configurado para efectuar una verificación sobre los datos transmitidos entre el puerto multifunciones $U_i$ y la interfaz INT, por lo tanto, entre el periférico P cuando está conectado a este puerto multifunciones $U_i$ y un sistema informático conectado a la interfaz INT.

Una verificación de este tipo puede hacerse, por ejemplo, limitando o modificando sobre la marcha los intercambios entre el puerto multifunciones $U_i$ y la interfaz INT, ya sea al nivel de los controles de bajo nivel (tipo lectura de la memoria con una dirección, toque de una tecla, adquisición de un valor o dato, etc.) o verificando los datos transportados respetan ciertas limitaciones, por ejemplo, que los caracteres transmitidos pertenecen ciertamente a un alfabeto dado, verificando que las líneas de datos responden ciertamente a ciertas características predefinidas, verificado una firma realizada sobre los datos transmitidos, etc...

Esta verificación puede tratar sobre todos los paquetes de datos intercambiados entre el puerto multifunciones $U_i$ y la interfaz INT, de forma más o menos evolucionada, por medio de una lista blanca, de un filtro de estado, de un filtro de memoria (según los intercambios anteriores) o de una verificación sobre el tamaño de los paquetes o una firma digital, por ejemplo.

En caso de fracaso de esta verificación, en un modo de realización, los datos ya no se transmiten entre el periférico P y el sistema de informaciones y el acceso al sistema de informaciones se interrumpe, lo que permite ofrecer un nivel suplementario de control de acceso. En otro modo de realización, estos datos se modifican sobre la marcha para que se vuelvan inofensivos.

Se hace referencia ahora a la figura **2A** que ilustra un primer modo particular de realización del dispositivo de control de acceso de la figura 1 que solo comprende dos puertos multifunciones.

En este primer modo particular de realización, el dispositivo de control de acceso DISP2 ilustrado toma la forma de una tarjeta PCI que hay que instalar en una carcasa de ordenador personal, con una interfaz PCI que sirve para la conexión con la placa base PB del ordenador personal.

Este dispositivo DISP2 comprende un primer puerto multifunciones $USB_1$, de tipo USB y un segundo puerto multifunciones $USB_2$, de tipo USB.

Los medios de gestión de acceso $M_{acc}$ del dispositivo DISP2 están entonces configurados físicamente, como se ha indicado anteriormente, para permitir el acceso de la interfaz PCI por medio de un periférico KB, cuando está conectado al primer puerto multifunciones $USB_1$, solamente si este periférico KB pertenece a una primera categoría $CP_1$ de periféricos asociada específicamente y de forma permanente al primer puerto multifunciones $USB_1$, en este caso la categoría de los teclados de ordenador.

Los medios de gestión de acceso $M_{acc}$ del dispositivo DISP2 están igualmente configurados físicamente para permitir el acceso de la interfaz PCI por medio de un periférico MS, cuando está conectado al segundo puerto multifunciones $USB_2$, solamente si este periférico MS pertenece a una segunda categoría $CP_2$ de periféricos asociada específicamente y de forma permanente al segundo puerto multifunciones $USB_2$ y distinta de la primera categoría $CP_1$ de periféricos, en este caso la categoría de los ratones de ordenador.*

En este modo de realización, los medios de acceso $M_{acc}$ consisten, por lo tanto, en un solo módulo de gestión de acceso común a los dos puertos multifunciones $USB_1$ y $USB_2$. De este modo, cuando un ordenador personal solo dispone de un dispositivo DISP2 de este tipo para comunicare con los usuarios, solo se aceptan unos teclados de tipo USB sobre el primer puerto $USB_1$ y solo se aceptan unos ratones de tipo USB sobre el segundo puerto $USB_2$, lo que impide, por ejemplo, la conexión de llaves USB para recuperar unos datos sensibles o de cables de red de tipo USB para intentar tomar el controlador de este ordenador personal.

Se hace referencia ahora a la **figura 2B** que ilustra un segundo modo particular de realización del dispositivo de control de acceso de la figura 1 que solo comprende tres puertos multifunciones.

En este segundo modo particular de realización, el dispositivo de control de acceso DISP3 ilustrado toma también la forma de una tarjeta PCI que hay que instalar en una carcasa de ordenador personal, con una interfaz PCI que sirve para la conexión con la placa base PB del ordenador personal.

Este dispositivo DISP3 comprende un primer puerto multifunciones $USB_1$, un segundo puerto multifunciones $USB_2$ y un tercer puerto multifunciones $USB_3$, todos de tipo USB.

Los medios de gestión de acceso $M_{acc}$ del dispositivo DISP3 están entonces configurados físicamente, como se ha indicado anteriormente, para permitir el acceso de la interfaz PCI por medio de un periférico KB, cuando está conectado al primer puerto multifunciones $USB_1$, solamente si este periférico KB pertenece a una primera categoría $CP_1$ de periféricos asociada específicamente y de forma permanente al primer puerto multifunciones $USB_1$, en este caso la categoría de los teclados de ordenador.

Los medios de gestión de acceso $M_{acc}$ del dispositivo DISP3 están igualmente configurados físicamente para permitir el acceso de la interfaz PCI por medio de un periférico MS, cuando está conectado al segundo puerto multifunciones $USB_2$, solamente si este periférico MS pertenece a una segunda categoría $CP_2$ de periféricos asociada específicamente y de forma permanente al segundo puerto multifunciones $USB_2$ y distinta de la primera categoría $CP_1$ de periféricos, en este caso la categoría de los ratones de ordenador.

Los medios de gestión de acceso $M_{acc}$ del dispositivo DISP3 están finalmente configurados físicamente para permitir el acceso de la interfaz PCI por medio de un periférico USBKY, cuando está conectado al tercer puerto multifunciones $USB_3$, solamente si este periférico USBKY pertenece a una tercera categoría $CP_3$ de periféricos asociada específicamente y de forma permanente al tercer puerto multifunciones $USB_3$ y distinta de las primera y segunda categorías de periféricos $CP_1$ y $CP_2$, en este caso la categoría de las llaves de almacenamiento USB.

En este modo de realización, los medios de acceso $M_{acc}$ consisten, por lo tanto, en un solo módulo de gestión de acceso común a los tres puertos multifunciones $USB_1$, $USB_2$ y $USB_3$.

De este modo, cuando un ordenador personal solo dispone de un dispositivo DISP3 de este tipo para comunicarse con los usuarios, solo se aceptan unos teclados de tipo USB sobre el primer puerto $USB_1$, solo se aceptan unos ratones de tipo USB sobre el segundo puerto $USB_2$ y solo se aceptan unas llaves de tipo USB sobre el tercer puerto $USB_3$.

Esto impide, por ejemplo, la conexión de cables de red de tipo USB para intentar tomar el control de este ordenador personal, permitiendo al mismo tiempo el almacenamiento de datos, opción que no ofrece el dispositivo DISP2 ilustrado en la figura 2A.

En la medida en que la conexión de llave de almacenamiento USB es posible con el dispositivo DISP3, se ofrece un grado menor de seguridad física con este dispositivo y puede ser ventajoso entonces emplear un módulo de verificación similar al módulo $M_{VERIF}$ descrito en relación con la figura 1, con el fin de efectuar un control sobre los datos transmitidos entre la interfaz PCI y una llave USBKY conectada al tercer puerto $USB_3$.

Se hace referencia ahora a la **figura 2C** que ilustra un tercer modo particular de realización del dispositivo de control de acceso de la figura 1 que comprende igualmente tres puertos multifunciones.

En este tercer modo particular de realización que se refiere a un dispositivo DISP3' que comprende una interfaz $INT_3$, un primer puerto multifunciones $USB_1$, de tipo USB, dedicado a la conexión de un periférico KB de tipo teclado, un segundo puerto multifunciones $USB_2$, de tipo USB, dedicado a la conexión de un periférico MS de tipo ratón y un tercer puerto multifunciones $USB_3$, de tipo USB, dedicado a la conexión de un periférico USBKY de tipo llave de almacenamiento, los medios de gestión de acceso $M_{acc}$ comprenden un primer módulo de gestión de acceso $M_{acc1}$, un segundo módulo de gestión de acceso $M_{acc2}$ y un tercer módulo de gestión de acceso $M_{acc3}$ asociados respectivamente a los puertos multifunciones $USB_1$, $USB_2$ y $USB_3$ y dedicados respectivamente a los tipos de periféricos de anteriormente.

En particular, el primer módulo de gestión de acceso $M_{acc1}$ comprende un módulo de tratamiento $FPGA_1$, conectado al puerto multifunciones $USB_1$ y configurado para efectuar la gestión del acceso, así como la verificación mencionadas anteriormente sobre los datos que emanan de un periférico KB y que transitan por este puerto $USB_1$, así como un puerto USB interno, designado por $USB'_1$ y conectado al módulo de tratamiento $FPGA_1$. Los datos que emanan del periférico KB y verificados en este primer módulo de gestión de acceso $M_{acc1}$ están disponibles de este modo a la salida de este módulo sobre el puerto USB interno $USB'_1$.

Este módulo de tratamiento $FPGA_1$ está configurado de este modo físicamente, como se ha indicado anteriormente, para permitir el acceso de la interfaz $INT_3$ por medio de un periférico KB, cuando está conectado al primer puerto multifunciones $USB_1$, solamente si este periférico KB pertenece a una primera categoría $CP_1$ de periféricos asociada específicamente y de forma permanente al primer puerto multifunciones $USB_1$, en este caso la categoría de los teclados de ordenador.

De manera similar, el segundo módulo de gestión de acceso $M_{acc2}$ comprende un módulo de tratamiento $FPGA_2$, conectado al puerto multifunciones $USB_2$ y configurado por efectuar la verificación mencionada anteriormente sobre los datos que emanan de un periférico MS y que transitan por este puerto $USB_2$, así como un puerto USB interno, designado por $USB'_2$ y conectado al módulo de tratamiento $FPGA_2$. Los datos que emanan del periférico MS y verificados en este segundo módulo de gestión de acceso $M_{acc2}$ están disponibles de este modo a la salida de este módulo sobre el puerto USB interno $USB'_2$.

Este módulo de tratamiento $FPGA_2$ está configurado de este modo físicamente, como se ha indicado anteriormente, para permitir el acceso de la interfaz $INT_3$ por medio de un periférico MS, cuando está conectado al segundo puerto multifunciones $USB_2$, solamente si este periférico MS pertenece a una segunda categoría $CP_2$ de periféricos asociada específicamente y de forma permanente al segundo puerto multifunciones $USB_2$, en este caso la categoría de los ratones.

Finalmente, el tercer módulo de gestión de acceso $M_{acc3}$ comprende un primer módulo de tratamiento $CPU_3$ conectado al puerto multifunciones $USB_3$, un segundo módulo de tratamiento $FPGA_3$ conectado al primer módulo de tratamiento $CPU_3$, así como un puerto USB interno, designado por $USB'_3$ y conectado al segundo módulo de tratamiento $FPGA_3$.

El segundo módulo de tratamiento $FPGA_3$ está configurado físicamente, como se ha indicado anteriormente, para permitir el acceso de la interfaz $INT_3$ por medio de un periférico USBKY, cuando está conectado al tercer puerto multifunciones $USB_3$, solamente si este periférico USBKY pertenece a una tercera categoría $CP_3$ de periféricos asociada específicamente y de forma permanente al tercer puerto multifunciones $USB_3$, en este caso la categoría de los periféricos de almacenamiento como, por ejemplo, las llaves de almacenamiento USB. Este segundo módulo de tratamiento $FPGA_3$ está configurado de este modo para efectuar la función de identificación de la categoría del periférico conectado al puerto multifunciones $USB_3$ y, por lo tanto, hace la función de módulo de identificación $M_{id}$ en el sentido de lo que se ha descrito anteriormente.

El primer módulo de tratamiento $CPU_3$ está, por su parte, configurado para efectuar la verificación de datos intercambiados por mediación del puerto $USB_3$ de la forma mencionada anteriormente. Este primer módulo de tratamiento $CPU_3$, por lo tanto, hace la función de módulo de verificación $M_{VERIF}$ en el sentido de lo que se ha descrito anteriormente.

De este modo, cuando un ordenador personal solo dispone de un dispositivo DISP3' de este tipo para comunicarse con los usuarios, solo se aceptan unos teclados de tipo USB sobre el primer puerto $USB_1$, solo se aceptan unos ratones de tipo USB sobre el segundo puerto $USB_2$ y solo se aceptan unas llaves de tipo USB sobre el tercer puerto $USB_3$.

En este caso, a diferencia del segundo modo de realización, el dispositivo DISP3' comprende una interfaz $INT_3$ que comprende ella misma un módulo hub USB, conectado a los puertos internos $USB_1$, $USB_2$ y $USB_3$, con el fin de gestionar los intercambios de datos entre estas diferentes interfaces. La interfaz $INT_3$ comprende igualmente una interfaz PCI para permitir la conexión del dispositivo DISP3' sobre una placa base PB y los intercambios de datos entre esta placa base y los puertos multifunciones.

La utilización de una interfaz $INT_3$ con un módulo hub USB permite optimizar los intercambios internos de datos entre los diferentes módulos de gestión de acceso y el sistema informático al que está conectado el dispositivo DISP3'.

El hub USB de la interfaz $INT_3$ puede conectarse, además, con otra interfaz USB interna $USB'_4$, que permite el intercambio de datos no filtrado con el sistema informático en el que está instalado el dispositivo DISP3'.

En el dispositivo DISP3', la verificación solo se efectúa sobre los datos intercambiados con un periférico de almacenamiento conectado al puerto $USB_3$ y no sobre los datos recibidos de los puertos $USB_1$ y $USB_2$, lo que permite optimizar la disposición interna del dispositivo y evitar unas verificaciones inútiles.

Finalmente, se hace referencia a la **figura 3** que ilustra las etapas de un procedimiento de acceso controlado a un sistema informático según la presente invención.

Un procedimiento de este tipo 100 de acceso controlado utiliza un dispositivo de control de acceso DISP, tal como se ha descrito en relación con la figura 1, que comprende un cierto número de puertos multifunciones $U_1$,..., $U_i$ que sirven para la conexión de periféricos distintos, una interfaz de acceso INT que sirve para la conexión al sistema informático considerado y unos medios de gestión de acceso $M_{acc}$, conectados entre los puertos multifunciones $U_1$,..., $U_i$ y la interfaz de acceso INT, que gestiona la conexión entre los puertos multifunciones $U_1$,..., $U_i$ y la interfaz de acceso INT.

El procedimiento 100 de acceso controlado puede comenzar por una etapa previa 110 de asociación física

permanente de una categoría específica de periféricos $CP_1$,..., $CP_i$ respectivamente a cada uno de dichos al menos un puerto multifunciones $U_1$,..., $U_i$ del dispositivo DISP, siendo estas diferentes categorías específicas de periféricos $CP_1$,..., $CP_i$ distintas las unas de las otras.

Como se ha indicado anteriormente, esta asociación física permanente puede realizarse programando los medios de gestión de acceso $M_{acc}$ en forma de un circuito programable, de tipo FPGA, que no puede modificarse ya después de programación de este circuito.

Esto permite fijar físicamente las diferentes categorías específicas de periféricos $CP_1$,..., $CP_i$ asociadas respectivamente a los puertos multifunciones $U_1$,..., $U_i$ y, por lo tanto, impedir que un usuario malicioso modifique una asociación de este tipo, lo que puede ser el caso con una aplicación no física de tipo software.

Como continuación a la conexión de un periférico P sobre uno de los puertos multifunciones $U_i$ (etapa 115 de conexión), el procedimiento 100 comprende la verificación (etapa 120) del hecho de que el periférico P pertenezca ciertamente a la categoría $CP_i$ de periféricos asociada específicamente y de forma permanente al puerto multifunciones $U_i$ al que está conectado este periférico P.

Si ciertamente el caso es de este tipo y solamente en este caso, se permite el acceso (etapa de permiso 130) por los medios de acceso $M_{acc}$, para este periférico P, a la interfaz INT del dispositivo DISP y, por lo tanto, al sistema informático al que está conectada esta interfaz INT. La etapa 130 de permiso de acceso puede comprender entonces la transferencia de datos entre el periférico P y el sistema informático IS en cuestión, mediante el puerto multifunciones $U_i$, los medios de gestión de acceso $M_{acc}$ y la interfaz de acceso INT del dispositivo DISP.

Si no, es decir, cuando el periférico P no pertenece a la categoría $CP_i$ de periféricos asociada específicamente y de forma permanente al puerto multifunciones $U_i$ al que está conectado este periférico P, se rechaza y bloquea el acceso del periférico P a la interfaz INT del dispositivo DISP por los medios de acceso $M_{acc}$ del dispositivo DISP.

En un modo de realización particular, el procedimiento 100 comprende, después de la conexión del periférico P al puerto multifunciones $U_i$, la identificación (etapa 121) de la categoría CP de este periférico P por el dispositivo DISP (más particularmente por un módulo de identificación $M_{id}$ comprendido en sus medios de acceso $M_{acc}$), se permite entonces el acceso a la interfaz de acceso INT en función de la comparación de la categoría CP identificada y de la categoría $CP_i$ de periféricos asociada específicamente y de forma permanente al puerto multifunciones $U_i$ (etapa 123 de comparación).

Si la categoría CP identificada corresponde a la categoría $CP_i$ de periféricos asociada específicamente y de forma permanente al puerto multifunciones $U_i$ y solamente en este caso, el acceso del periférico P a la interfaz INT del dispositivo DISP y, por lo tanto, al sistema informático al que está conectada esta interfaz INT, se permite por los medios de acceso $M_{acc}$. (etapa de permiso 130).

Si, por contra, la categoría CP identificada no corresponde a la categoría $CP_i$ de periféricos asociada específicamente y de forma permanente al puerto multifunciones $U_i$, se rechaza y bloquea el acceso del periférico P a la interfaz INT del dispositivo DISP por los medios de acceso $M_{acc}$ del dispositivo DISP.

En un modo de realización ventajoso, el procedimiento 100 de acceso controlado comprende, además, la verificación (etapa 140) de los datos transmitidos, después de la etapa 130 de permiso de acceso, entre el puerto multifunciones $U_i$ al que está conectado el periférico y la interfaz INT del dispositivo DISP conectado al sistema informático IS.

Esta verificación puede hacerse por un módulo de verificación $M_{verif}$ tal como se ha descrito anteriormente y puede comprender, por ejemplo, la verificación del hecho de que los caracteres transmitidos pertenezcan ciertamente a un alfabeto dado, que las líneas de datos respondan ciertamente a ciertas características predefinidas o la verificación de una firma efectuada sobre los datos transmitidos, etc.

Si el resultado de esta verificación es positivo, el periférico P puede comunicarse e intercambiar unos datos con un sistema informático conectado a la interfaz INT mediante el puerto multifunciones $U_i$, los medios de acceso $M_{acc}$ y la interfaz de acceso INT del dispositivo DISP.

Si el resultado de esta verificación es negativo, la transferencia de datos entre el periférico P y la interfaz de acceso INT del dispositivo DISP se interrumpe por los medios de gestión de acceso $M_{acc}$ (etapa 145 de interrupción de transferencia de datos).

La presente invención tiene como objeto, además, un programa de ordenador que incluye unas instrucciones de código para la implementación del procedimiento de control de acceso descrito anteriormente cuando este programa se ejecuta por el procesador de un dispositivo de control de acceso, por ejemplo, por el procesador PROC situado en los módulos de identificación $M_{id}$ del dispositivo DISP descrito en la figura 1.

Un programa de este tipo puede utilizar cualquier lenguaje de programación y estar en forma de un código fuente, código objeto o de código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada o en cualquier otra forma deseable.

La presente invención también tiene como objeto un soporte de informaciones legible por un ordenador o un procesador de datos y que incluye unas instrucciones de código del programa mencionado más arriba. Este soporte de informaciones puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como un ROM, por ejemplo, un CD-ROM o un ROM de circuito microelectrónico o también un medio de grabación magnético, por ejemplo, un disquete o un disco duro. Este soporte de informaciones puede incluir igualmente memoria tipo FLASH, para el almacenamiento del programa y la grabación de las informaciones recepcionadas por un módulo cliente y memoria de tipo RAM para la salvaguarda de los datos temporales tales como las listas de servidores y temas asociados.

Por otra parte, este soporte de informaciones puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede conducirse mediante un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede descargarse, en particular, en una red de tipo Internet.

Por supuesto, la invención no se limita a los ejemplos de realización de más arriba descritos y representados, a partir de los que se podrán prever otros modos y otras formas de realización, sin, no obstante, salirse del marco de la invención, que se define por las siguientes reivindicaciones.

**REIVINDICACIONES**

1. Dispositivo de control de acceso a un sistema informático, comprendiendo el dispositivo al menos un puerto multifunciones adecuado para conectarse a diferentes categorías de periféricos y una interfaz de acceso adecuada para conectarse al sistema informático, comprendiendo el dispositivo unos medios de gestión de acceso conectados, por mediación de un controlador, entre el puerto multifunciones y la interfaz y configurados físicamente para permitir un acceso de la interfaz por medio de un periférico conectado al puerto multifunciones solamente si dicho periférico pertenece a una categoría de periféricos asociada específicamente y de forma permanente al puerto multifunciones al que está conectado, estando el dispositivo **caracterizado por que**:

los medios de gestión de acceso comprenden un módulo de identificación que permite identificar una categoría del periférico conectado al puerto multifunciones interceptando unos datos de descripción de aparato intercambiados sobre el controlador durante una conexión de este periférico.

2. Dispositivo según la reivindicación 1, **caracterizado por que** comprende un primer y un segundo puertos multifunciones y **por que** los medios de gestión de acceso están configurados físicamente para permitir el acceso de la interfaz por medio de un periférico conectado al primer puerto multifunciones solamente si dicho periférico pertenece a una primera categoría de periféricos asociada específicamente y de forma permanente al primer puerto multifunciones y para permitir el acceso de la interfaz por medio de un periférico conectado al segundo puerto multifunciones solamente si dicho periférico pertenece a una segunda categoría de periféricos asociada específicamente y de forma permanente al segundo puerto multifunciones y distinta de la primera categoría de periféricos.

3. Dispositivo según la reivindicación 2, **caracterizado por que** comprende, además, un tercer puerto multifunciones y **por que** los medios de gestión de acceso están configurados físicamente para permitir el acceso de la interfaz por medio de un periférico conectado al tercer puerto multifunciones solamente si dicho periférico pertenece a una tercera categoría de periféricos asociada específicamente y de forma permanente al tercer puerto multifunciones y distinta de las primera y segunda categorías de periféricos.

4. Dispositivo según la reivindicación 3, **caracterizado por que** los medios de gestión de acceso comprenden un primer módulo de acceso, un segundo módulo de acceso y un tercer módulo de acceso conectados respectivamente al primer puerto multifunciones, al segundo puerto multifunciones y al tercer puerto multifunciones y **por que** la interfaz de acceso comprende un módulo hub conectado a dichos primero, segundo y tercer módulo de acceso.

5. Dispositivo según una de las reivindicaciones 1 a 4, **caracterizado por que** los medios de gestión de acceso comprenden unos medios de memorización que memorizan la categoría de periféricos asociada específicamente y de forma permanente a dicho puerto multifunciones.

6. Dispositivo según una cualquiera de las reivindicaciones 1 a 5, **caracterizado por que** los medios de gestión de acceso comprenden, además, un módulo de verificación, conectado entre los medios de gestión de acceso y la interfaz, configurado para efectuar una verificación sobre los datos transmitidos entre el puerto multifunciones y la interfaz.

7. Dispositivo según una de las reivindicaciones 1 a 6, **caracterizado por que** los medios de gestión de acceso incluyen unos circuitos programables una única vez.

8. Dispositivo según una cualquiera de las reivindicaciones 1 a 7, **caracterizado por que** una primera, una segunda y/o una tercera categoría de periféricos corresponden a una categoría de periféricos de entre los teclados, los ratones y las llaves de almacenamiento.

9. Dispositivo según una cualquiera de las reivindicaciones 1 a 8, **caracterizado por que** al menos un puerto multifunciones es un puerto universal de tipo USB.

10. Procedimiento de control de acceso de un periférico a un sistema informático por medio de un dispositivo de control de acceso que comprende un puerto multifunciones al que está conectado el periférico y una interfaz a la que está conectado el sistema informático, comprendiendo el procedimiento:

- identificación de una categoría asociada al periférico conectado al puerto multifunciones, permitiéndose un acceso a la interfaz solamente si la categoría identificada corresponde a una categoría de periféricos específicamente asociada al puerto multifunciones al que está conectado el periférico; y
- permiso de acceso, para el periférico, a la interfaz conectada al sistema informático solamente si dicho periférico pertenece a una categoría de periféricos asociada específicamente y de forma permanente al puerto multifunciones al que está conectado dicho periférico, estando el procedimiento **caracterizado por que**:

la identificación de la categoría se basa en la interceptación de los datos de descripción de aparato intercambiados sobre el controlador durante una conexión de este periférico.

11. Procedimiento según la reivindicación 10, **caracterizado por** la verificación de los datos transmitidos, después del permiso de acceso, entre el puerto multifunciones al que está conectado el periférico y la interfaz del dispositivo conectada al sistema informático.

12. Procedimiento según una cualquiera de las reivindicaciones 10 u 11, **caracterizado por** una etapa previa de asociación física permanente de una categoría específica de periféricos respectivamente a cada uno de dichos al menos un puerto multifunciones del dispositivo, siendo dichas categorías específicas de periféricos distintas las unas de las otras.

13. Programa de ordenador que incluye unas instrucciones de código para la implementación del procedimiento de control de acceso según una de las reivindicaciones 10 a 12, cuando este programa se ejecuta por el procesador de un dispositivo de control de acceso que conecta un periférico a un sistema informático.

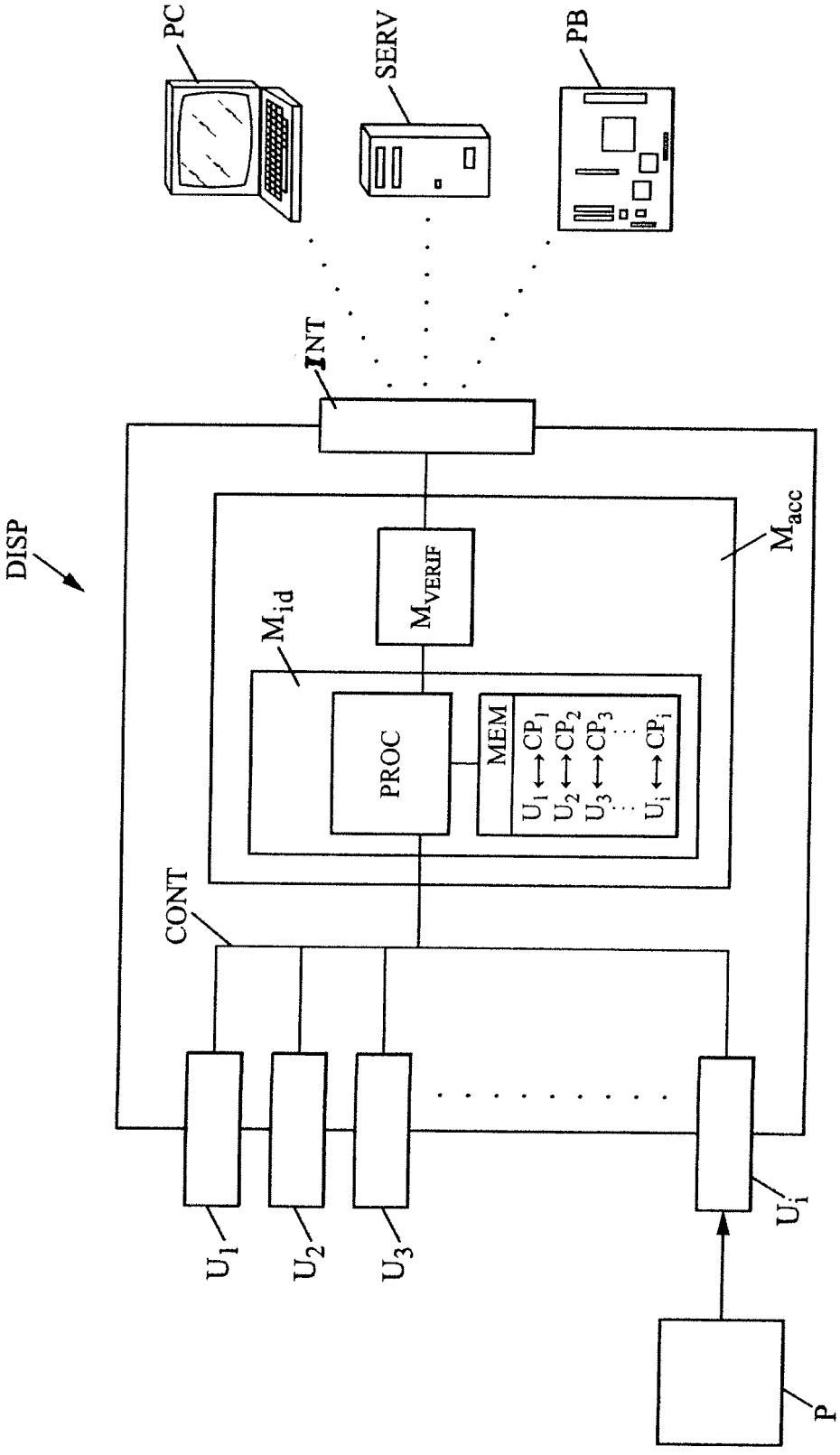
PC
SERV
PB
INT
DISP
$M_{acc}$
$M_{VERIF}$
$M_{id}$
PROC
MEM
$U_1 \leftrightarrow CP_1$
$U_2 \leftrightarrow CP_2$
$U_3 \leftrightarrow CP_3$
$U_i \leftrightarrow CP_i$
CONT
$U_1$
$U_2$
$U_3$
$U_i$
P

FIG. 1

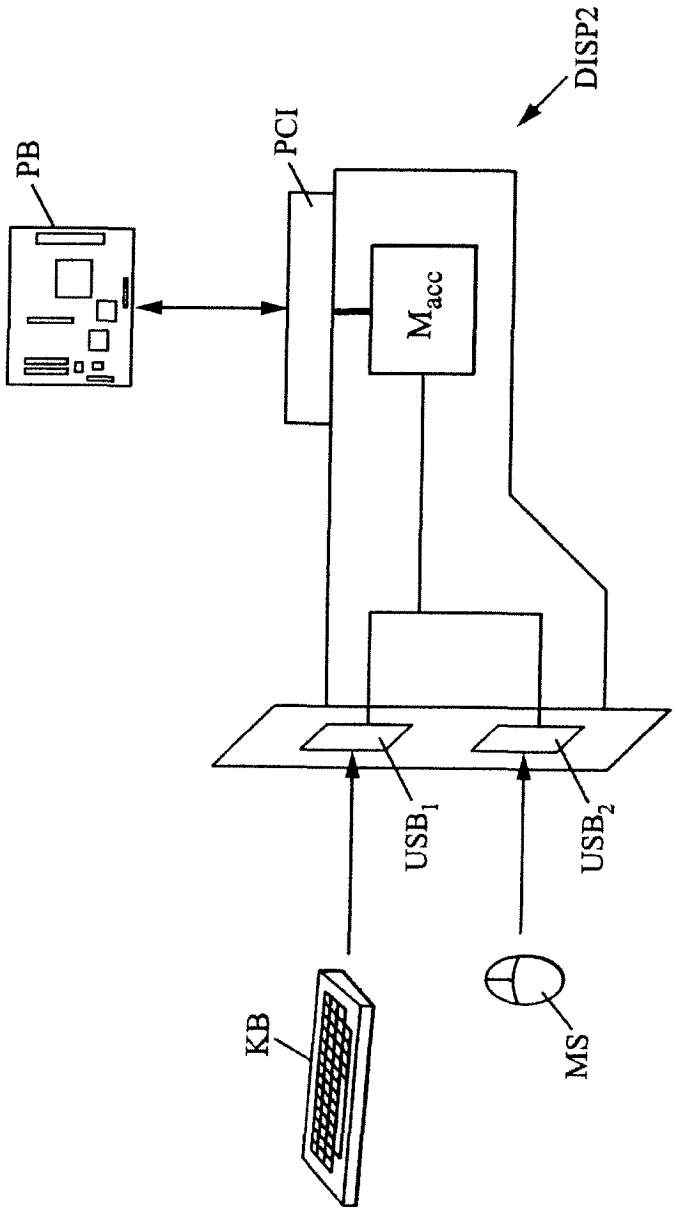


FIG. 2A

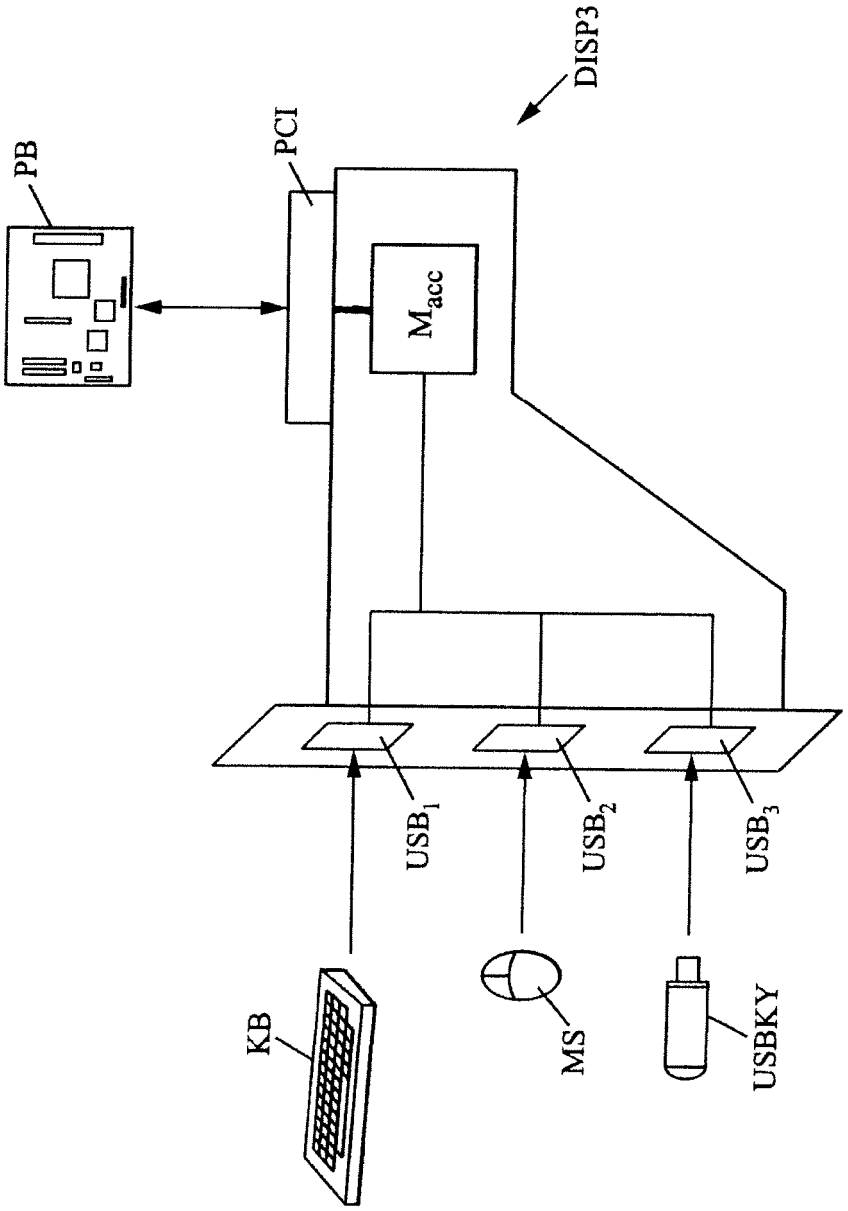


FIG. 2B

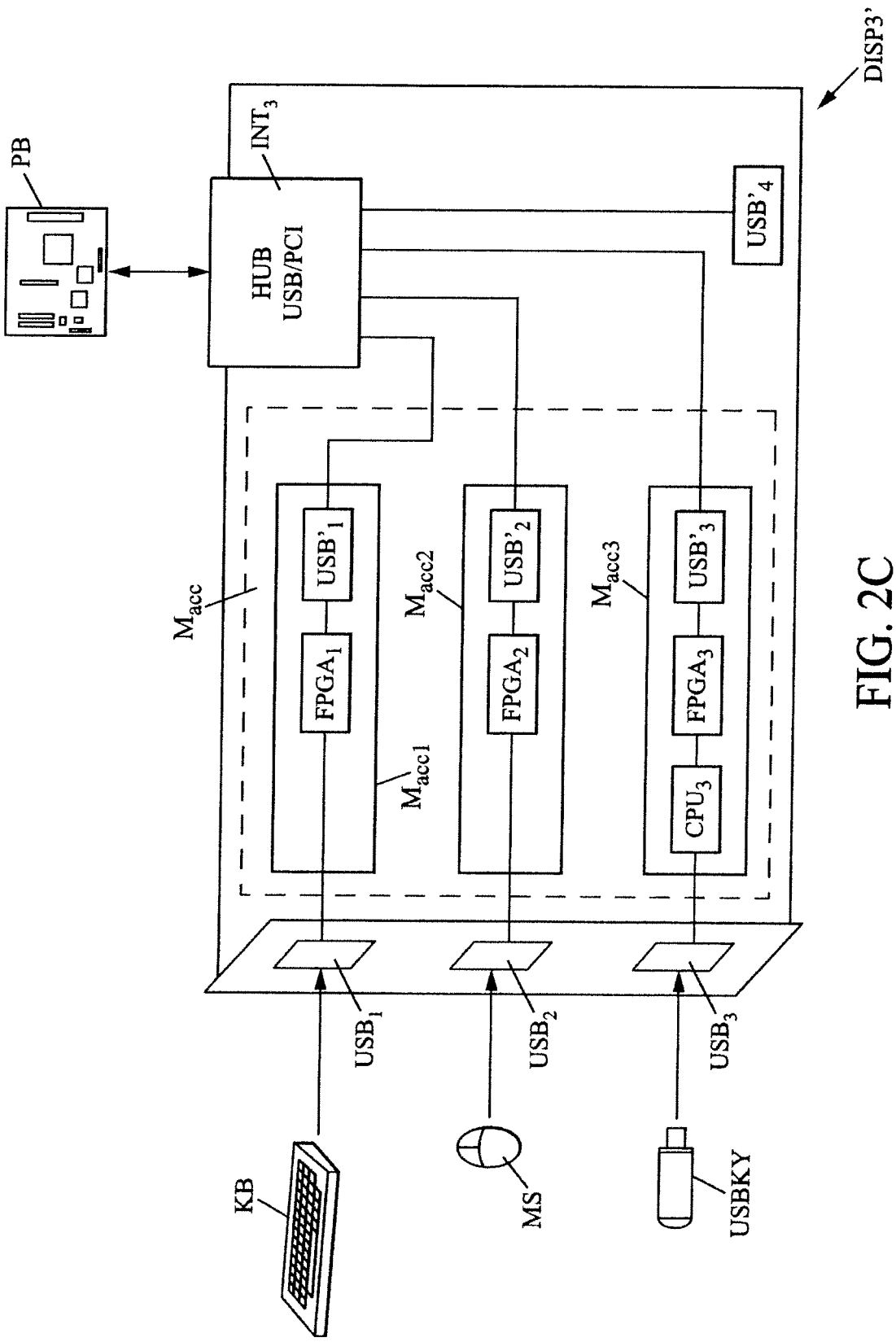
DISP3'
PB
INT3
HUB
USB/PCI
USB'4
Macc
Macc1
Macc2
Macc3
USB'1
USB'2
USB'3
FPGA1
FPGA2
FPGA3
CPU3
USB1
USB2
USB3
KB
MS
USBKY

FIG. 2C

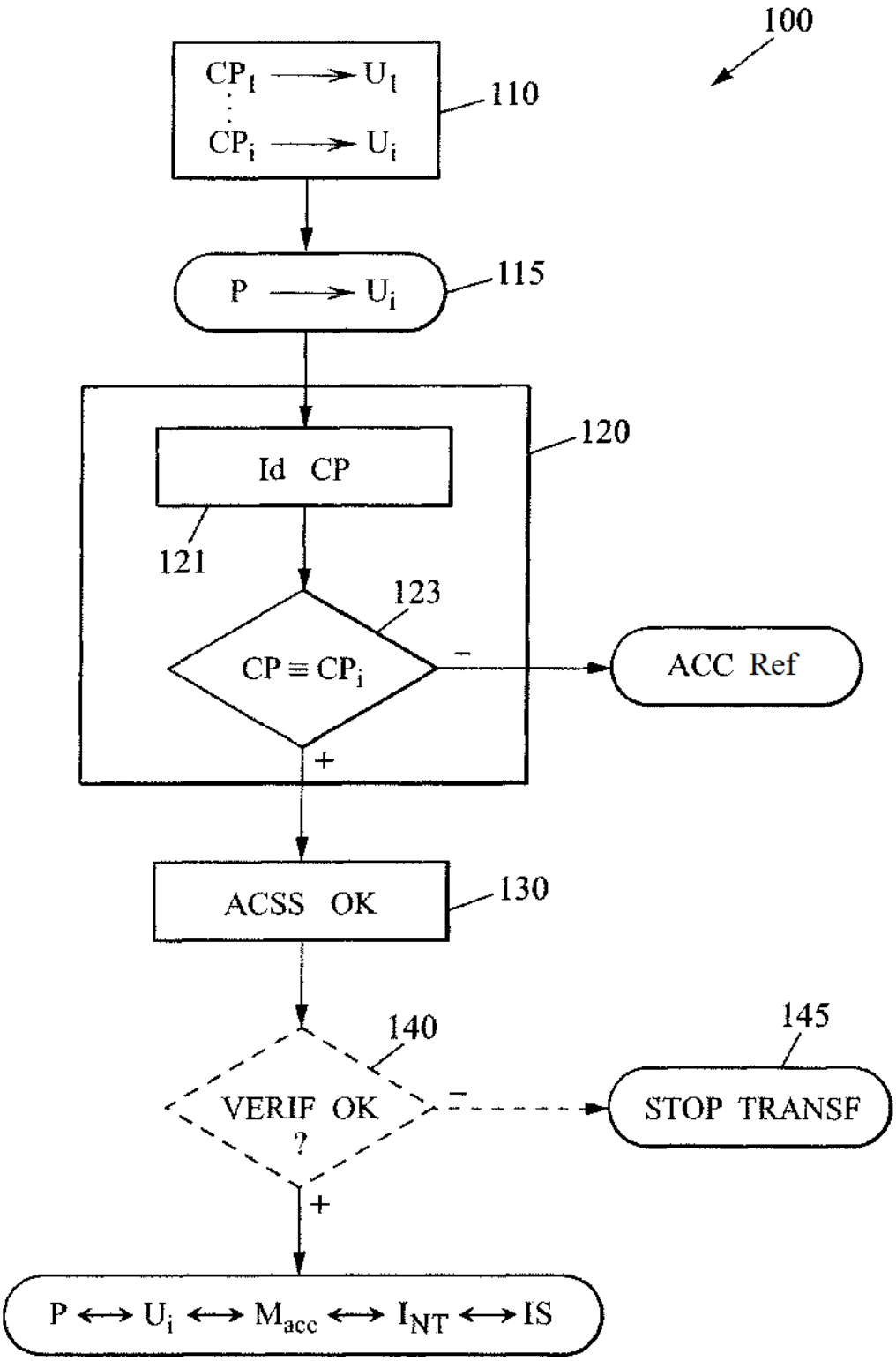
100
CP1 → U1
CPi → Ui
110
P → Ui
115
120
Id CP
121
123
CP ≡ CPi
–
ACC Ref
+
ACSS OK
130
140
145
VERIF OK ?
–
STOP TRANSF
+
P ↔ Ui ↔ Macc ↔ INT ↔ IS

FIG. 3