(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 693 450**

(51) Int. CI.:

G06F 21/78 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.06.2009 E 09161673 (0)**

(97) Fecha y número de publicación de la concesión europea: **01.08.2018 EP 2131300**

(54) Título: **Procedimiento y dispositivo de protección para entidad electrónica portátil**

(30) Prioridad:

06.06.2008 FR 0853793

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.12.2018

(73) Titular/es:

IDEMIA FRANCE (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

MOYART, DIDIER y
LEDUC, OLIVIER

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento y dispositivo de protección para entidad electrónica portátil

La presente invención se refiere a los periféricos para unidades de procesamiento tales como llaves USB, tarjetas de tipo MMC o SD y lectores de dichas tarjetas y más particularmente a un procedimiento y un dispositivo que permitan proteger los datos contenidos en dichos periféricos o accesibles a través de dichos periféricos.

Existen numerosos periféricos, actualmente utilizados, tales como las llaves USB (siglas de *Universal Serial Bus* en terminología anglosajona), tarjetas de tipo MMC (siglas de *Multimedia Memory Card* en terminología anglosajona) y SD (siglas de *Secure Digital* en terminología anglosajona), las tarjetas de microcircuitos, principalmente las tarjetas de microcircuitos de acuerdo con la norma ISO 7816, y los lectores de dichas tarjetas, permiten añadir funcionalidades a una unidad de procesamiento, por ejemplo funcionalidades de almacenamiento.

Las unidades de procesamiento, también llamadas estaciones huésped, adaptadas para cooperar con dichos periféricos, son principalmente los ordenadores, los teléfonos móviles y los asistentes personales también llamados PDA (siglas de *Personal Digital Assistant* en terminología anglosajona). Las conexiones entre estas unidades de procesamiento y los periféricos se realizan de manera clásica, principalmente con ayuda de una interfaz física y de un enlace eléctrico, o según una tecnología inalámbrica, por ejemplo según la normas denominadas *wireless USB* en terminología anglosajona.

Ciertos periféricos implementan dispositivos para proteger el acceso a las funciones de los periféricos o a los datos memorizados en estos últimos. Existen también sistemas USB que comprenden varias subinterfaces, principalmente de tipo de almacenamiento y de tipo interfaz de usuario. Dichos sistemas están adaptados para implementar funciones de seguridad de tal manera que las zonas de almacenamiento no sean accesibles efectivamente más que después de la autentificación del usuario.

Existen igualmente periféricos que comprenden módulos de cifrado y de descifrado de datos que permiten cifrar todos los datos que deben memorizarse y descifrar todos los datos que deben leerse, después de la autentificación. Ciertos periféricos comprenden también microcontroladores que permiten gestionar los accesos a las memorias y que integran unas funciones de cifrado y de descifrado.

Sin embargo, dichos componentes son específicos y, en consecuencia, tienen costes importantes.

El documento US2007/113097A1 describe un soporte de almacenamiento que comprende un medio de la adaptación de características biológicas del usuario y una tarjeta de chips; en el que la función biológica de un usuario se utiliza como contraseña para acceder al soporte de almacenamiento y la tarjeta de chips se utiliza para cifrar / descifrar los datos almacenados en el soporte de almacenamiento con el fin de proteger eficazmente los datos almacenados en el soporte de almacenamiento.

El documento US2001/011267A1 describe la utilización de una tarjeta de memoria para gestionar ficheros registrados en una memoria no volátil con una tabla de asignación de ficheros (FAT). La invención permite resolver al menos uno de los problemas expuestos anteriormente combinando la protección de los datos y la utilización de componentes no específicos.

La invención tiene así por objeto un procedimiento para acceder a al menos un dato cifrado previamente memorizado en una memoria en masa de una entidad electrónica portátil o en una memoria en masa accesible a través de dicha entidad electrónica portátil, adaptada dicha entidad electrónica portátil para conectarse a una estación huésped, comprendiendo dicha entidad electrónica portátil unos medios de acceso a dicha memoria en masa que comprende dicho al menos un dato cifrado y unos medios de protección adaptados para descifrar dicho al menos un dato cifrado, siendo distintos e independientes dichos medios de acceso y dichos medios de protección y no intercambiando datos entre ellos, comprendiendo este procedimiento las siguientes etapas,

- recepción de dicho al menos un dato cifrado de dichos medios de acceso;
- transmisión de dicho al menos un dato cifrado recibido en dichos medios de protección para ser ahí descifrado; y,
- recepción de dicho al menos un dato descifrado,

implementándose dichas etapas en dicha estación huésped.

El procedimiento según la invención permite así implementar independientemente un circuito de protección y un controlador asociados a una memoria en masa para proteger los datos almacenados en esta memoria.

De manera ventajosa, el procedimiento comprende además una etapa de creación de una partición, comprendiendo dicha partición al menos dicho al menos un dato descifrado recibido.

Según un modo de realización particular, el procedimiento comprende además las siguientes etapas,

- transmisión de al menos una información de autentificación a dichos medios de protección; y,
- recepción de una indicación de autentificación,

implementándose dichas etapas en dicha estación huésped.

El procedimiento según la invención permite así autentificar al usuario.

Dicho al menos un dato descifrado no se recibe, preferentemente, más que después del autentificación para limitar su accesibilidad.

De manera ventajosa, dicha etapa de creación de partición no se realiza más que después de la autentificación de tal manera que la partición no sea visible si el usuario no está autentificado.

La invención tiene igualmente por objeto un procedimiento para memorizar al menos un dato de manera cifrada en una memoria en masa de una entidad electrónica portátil o en una memoria en masa accesible a través de dicha entidad electrónica portátil, adaptada dicha entidad electrónica portátil para conectarse a una estación huésped, comprendiendo dicha entidad electrónica portátil unos medios de acceso a dicha memoria en masa y unos medios de protección adaptados para cifrar dicho al menos un dato, siendo distintos e independientes dichos medios de acceso y dichos medios de protección y no intercambiando datos entre ellos, comprendiendo este procedimiento las siguientes etapas,

- transmisión de dicho al menos un dato a dichos medios de protección para ser ahí cifrado;
- recepción de dicho al menos un dato cifrado desde dichos medios de protección; y,
- transmisión de dicho al menos un dato cifrado a dichos medios de acceso para memorizar dicho al menos un dato cifrado en dicha memoria en masa,

implementándose dichas etapas en dicha estación huésped.

El procedimiento según la invención permite así implementar independientemente un circuito de protección y un controlador asociado a una memoria en masa para proteger los datos almacenados en esta memoria.

Según un modo de realización particular, el procedimiento comprende además una etapa de memorización de todos los datos de dicha partición creada. Dicha etapa de memorización de todos los datos se efectúa, preferentemente, automáticamente en el transcurso de un procedimiento de desconexión de dicha entidad electrónica portátil. Dicha etapa de memorización de todos los datos puede efectuarse igualmente bajo petición del usuario de dicha entidad electrónica portátil o de dicha estación huésped.

La invención tiene también por objeto un procedimiento para acceder a al menos un dato cifrado previamente memorizado en una memoria en masa de una entidad electrónica portátil o en una memoria en masa accesible a través de dicha entidad electrónica portátil, adaptada dicha entidad electrónica portátil para conectarse a una estación huésped, comprendiendo dicha entidad electrónica portátil unos medios de acceso a dicha memoria en masa que comprende dicho al menos un dato cifrado y unos medios de protección adaptados para descifrar dicho al menos un dato, siendo distintos e independientes dichos medios de acceso y dichos medios de protección y no intercambiando datos entre ellos, comprendiendo este procedimiento las siguientes etapas,

- recepción de una solicitud de acceso a dicho al menos un dato cifrado por dichos medios de acceso;
- transmisión de dicho al menos un dato cifrado a dicha estación huésped;
- recepción de dicho al menos un dato cifrado por dichos medios de protección;
- descifrado de dicho al menos un dato cifrado; y,
- transmisión de dicho al menos un dato descifrado a dicha estación huésped.

El procedimiento según la invención permite así implementar independientemente un circuito de protección y un controlador asociado a una memoria en masa para proteger los datos almacenados en esta memoria.

La invención tiene igualmente por objeto un procedimiento para memorizar al menos un dato de manera cifrada en una memoria en masa de una entidad electrónica portátil o en una memoria en masa accesible a través de dicha entidad electrónica portátil, adaptada dicha entidad electrónica portátil para conectarse a una estación huésped, comprendiendo dicha entidad electrónica portátil unos medios de acceso a dicha memoria en masa y medios de protección adaptados para cifrar dicho al menos un dato, siendo distintos e independientes dichos medios de acceso y dichos medios de protección y no intercambiando datos entre ellos, este procedimiento se caracteriza por que comprende las siguientes etapas,

- recepción de dicho al menos un dato por dichos medios de protección;
- cifrado de dicho al menos un dato en dichos medios de protección;
- transmisión de dicho al menos un dato cifrado a dicha estación huésped;
- recepción de dicho al menos un dato cifrado desde dicha estación huésped por dichos medios de acceso; y,

- transmisión de dicho al menos un dato cifrado a dicha memoria en masa para ser ahí memorizado.

El procedimiento según la invención permite así implementar independientemente un circuito de protección y un controlador asociado a una memoria en masa para proteger los datos almacenados en esta memoria.

De manera ventajosa, el procedimiento comprende además una etapa de recepción de al menos una información de autentificación y una etapa de autentificación del usuario de dicha entidad electrónica portátil para limitar el acceso a dicho al menos un dato.

Según un modo de realización particular, dicha etapa de autentificación se implementa en dichos medios de protección.

De manera ventajosa, dichas etapas de descifrado y de transmisión de dicho al menos un dato descifrado no se ejecutan más que después de la autentificación de dicho usuario de dicha entidad electrónica portátil con el fin de controlar el acceso a dicho al menos un dato.

Dichas etapas de cifrado y de transmisión de dicho al menos un dato cifrado no se ejecutan ventajosamente más que después de la autentificación de dicho usuario de dicha entidad electrónica portátil para controlar los datos que deben memorizarse en dicha entidad electrónica portátil.

La invención tiene igualmente por objeto un programa de informático que comprende instrucciones adaptadas para la implementación de cada una de las etapas del procedimiento anteriormente descrito.

La invención tiene también por objeto un dispositivo para entidad electrónica portátil tal como se reivindica en la reivindicación 17 adjunta. El dispositivo según la invención permite de ese modo implementar independientemente un circuito de protección y un controlador asociado a una memoria en masa para proteger los datos almacenados en esta memoria.

De manera ventajosa, el dispositivo comprende además unos medios para recibir al menos una información de autentificación, comprendiendo dichos medios de protección unos medios de autentificación adaptados para autentificar a un usuario según al menos una información de autentificación recibida. Igualmente, dichos medios de protección comprenden unos medios de cifrado y de descifrado adaptados para cifrar unos datos a memorizar en dicha entidad electrónica y para descifrar unos datos memorizados en dicha entidad electrónica.

El dispositivo comprende además, ventajosamente, unos medios de almacenamiento adaptados para memorizar al menos una clave de cifrado y/o de descifrado utilizada para cifrar o descifrar unos datos a memorizar o memorizados en dicha entidad electrónica.

Según un modo de realización particular, el dispositivo comprende además unos medios de almacenamiento adaptados para memorizar un módulo de software de control, comprendiendo dicho módulo de software de control instrucciones adaptadas para implementar cada una de las etapas del procedimiento descrito anteriormente, pudiendo transmitirse a dicha estación huésped para ser ahí ejecutados. El dispositivo según la invención puede utilizarse así con una estación huésped sin que sea necesario instalar previamente un módulo de software específico.

De manera ventajosa, el dispositivo comprende además unos medios de almacenamiento adaptados para memorizar un módulo de software de protección, comprendiendo dicho módulo de software de protección instrucciones adaptadas para implementar cada una de las etapas del procedimiento descrito anteriormente, pudiendo ser ejecutadas por dichos medios de protección. El dispositivo según la invención puede utilizarse así con una estación huésped sin necesidad de instalación de software particular.

Según un modo de realización particular, dicho dispositivo comprende además una memoria en masa que comprende dicha zona de memoria.

Siempre según un modo de realización particular, dichos medios de protección están integrados en una tarjeta de microcircuitos. Es posible así añadir y personalizar funcionalidades de protección de los datos en una entidad electrónica portátil.

La invención tiene igualmente por objeto una llave de tipo USB que comprende el dispositivo anteriormente descrito.

Surgirán otras ventajas, objetos y características de la presente invención de la descripción que se detalla a continuación, realizada a título de ejemplo no limitativo, con relación a los dibujos adjuntos en los que:

- la figura 1 representa un ejemplo de arquitectura de una entidad electrónica portátil según la invención;
- la figura 2 ilustra un ordenador al que puede conectarse la entidad electrónica portátil representada en la figura anterior;

- la figura 3 ilustra un ejemplo de algoritmo implementado en la estación huésped, después de la conexión de una entidad electrónica portátil de acuerdo con la invención, que permite acceder a unos datos cifrados en o a través de una entidad electrónica portátil de ese tipo;
- la figura 4 ilustra un ejemplo de algoritmo que puede ejecutarse por una entidad electrónica portátil de acuerdo con la invención, después de la conexión de esta a una estación huésped, para permitir a esta última acceder a unos datos cifrados en o a través de esta entidad electrónica portátil;
- la figura 5 ilustra un ejemplo de algoritmo implementado en una estación huésped para cifrar unos datos en una entidad electrónica portátil y memorizar estos datos en esta o a través de esta;
- la figura 6 ilustra un ejemplo de algoritmo que puede ejecutarse por una entidad electrónica portátil según la invención para permitir a una estación huésped transferir unos datos en o a través de esta entidad electrónica portátil, siendo memorizados estos datos en forma cifrada; y,
- la figura 7 ilustra un ejemplo de arquitectura de estación huésped adaptada para implementar la invención.

De manera general, la invención se refiere a una entidad electrónica portátil o de bolsillo que puede conectarse con ayuda de una interfaz física o inalámbrica a una estación huésped tal como un ordenador de tipo PC (siglas de *Personal Computer* en terminología anglosajona), un teléfono móvil o un asistente personal, que comprende una memoria en masa o adecuada para conectarse a una memoria en masa. La entidad electrónica portátil según la invención comprende unos medios para cifrar y descifrar al menos una parte de los datos memorizados.

La entidad electrónica portátil o de bolsillo puede ser por ejemplo, una tarjeta de tipo MMC o SD, una tarjeta de microcircuitos, principalmente una tarjeta de microcircuitos de conformidad con la norma ISO 7816, un lector USB de una de dichas tarjetas o una llave USB.

La entidad electrónica portátil dispone en este caso de una memoria en masa, formada, por ejemplo, por una memoria flash o por una memoria de tipo EEPROM (acrónimo de *Electrically-Erasable Programmable Read Only Memory* en terminología anglosajona), es decir una memoria no volátil borrable y programable eléctricamente, de un disco duro, de un lector, eventualmente grabador, de CD o cualquier otro componente conocido para el experto en la materia o de una interfaz hacia una de dichas memorias. La cantidad de memoria es superior, preferentemente, a 10 megabytes.

La entidad electrónica portátil incluye un controlador de memoria que permite acceder a la memoria en masa contenida en la entidad electrónica portátil o en una memoria en masa que puede conectarse a la entidad electrónica portátil.

La entidad electrónica portátil incluye igualmente un componente protegido, es decir un componente que incluye unos medios de cálculo criptográfico, unos medios de memorización adaptados para almacenar una clave secreta y unos medios de cifrado y de descifrado. Ventajosamente, el componente protegido comprende igualmente unos medios que ofrecen una protección contra ataques que se dirijan a obtener informaciones secretas como por ejemplo la clave, memorizadas en la entidad electrónica portátil.

El componente protegido es distinto del controlador de memoria. Puede integrarse, por ejemplo, en una tarjeta de microcircuitos, principalmente una tarjeta cuyo formato esté conforme con la norma ISO 7816. Una de dichas tarjetas puede ser extraíble o no, comprendiendo en este caso la entidad electrónica portátil un lector de tarjetas adaptadas.

La entidad electrónica portátil comprende además una interfaz de comunicación que permite conectarla a una estación huésped. Este interfaz de comunicación se une al controlador de memoria y al componente protegido. Alternativamente, la entidad electrónica portátil puede comprender dos interfaces de comunicación para establecer dos conexiones independientes entre el controlador de memoria y la estación huésped y entre el componente protegido y la estación huésped.

La figura 1 ilustra un ejemplo de una entidad electrónica portátil según la invención, en este caso una llave USB que comprende una memoria en masa de acceso protegido.

Como se ha ilustrado, la llave USB 100 comprende una memoria 105, por ejemplo una memoria flash, un controlador de memoria 110, una interfaz de comunicación 115, conectada en este caso a una interfaz física 120, y un microcontrolador protegido 125.

La interfaz de comunicación 115 permite, en particular, a la llave USB 100 ser identificada como un periférico de clase memoria, o MSC (siglas de *Mass Storage Class* en terminología anglosajona), de tipo memoria en masa, lector de CD-ROM (acrónimo de *Compact Disc Read Only Memory* en terminología anglosajona) o similar, de conformidad con la norma USB.

La interfaz de comunicación 115 está adaptada para implementar una funcionalidad de concentrador, también denominado *hub* en terminología anglosajona, que permite dirigir los mensajes recibidos al controlador de memoria 110 o al microcontrolador protegido 125. El direccionado puede efectuarse principalmente por medio de un indicador, por ejemplo el valor de un bit, contenido en los mensajes recibidos.

El microcontrolador protegido 125 comprende en sí mismo una unidad de cálculo 130 (CPU, siglas de *Central Processing Unit* en terminología anglosajona), una memoria no volátil 135 (ROM, acrónimo de *Read Only Memory* en terminología anglosajona), una memoria volátil o memoria caché 140 (RAM, acrónimo de *Random Access Memory* en terminología anglosajona) y memoria de tipo EEPROM.

Las memorias no volátil 135 y volátil 140 se utilizan de manera clásica por la unidad de cálculo 130.

La memoria 145 de tipo EEPROM está particularmente adaptada para memorizar una clave secreta y/o una contraseña tal como un código PIN (acrónimo de *Personal Identification Number* en terminología anglosajona).

Las funciones de cifrado y de descifrado pueden memorizarse en la memoria no volátil 135 o, ventajosamente, en la memoria 145 de tipo EEPROM. Se ha de observar que al ser esta última reescribible, permite actualizaciones de software.

La memoria 105 puede considerarse como una o varias particiones, es decir según la definición comúnmente admitida, como una memoria que comprende un sistema de gestión de archivos.

A título de ilustración, la memoria 105 comprende en este caso una partición 150 cuyos datos están cifrados. La partición 150 se almacena en este caso en la forma de un archivo cifrado.

La memoria 105 está adaptada para memorizar un módulo de software, denominado software de control en lo que sigue de la descripción, pudiendo transferirse a la estación huésped para ser ejecutado ahí. Alternativamente, el módulo de software puede memorizarse en la memoria 145.

Según un modo de realización particular, cuando la entidad electrónica portátil está conectada (y en trance de utilización) se considera como memoria en masa de la que al menos una partición está cifrada, es decir que al menos una partición representa unos datos “no inteligibles”.

La interfaz 120 de la llave USB 100 es en este caso una interfaz de conformidad con la norma USB que permite conectar la llave a una unidad de procesamiento tal como un ordenador. Alternativamente, si la interfaz de comunicación 115 es de tipo inalámbrico, la interfaz 120 es sustituida por una antena. La interfaz 115/120 puede consistir igualmente en una doble interfaz que permite una conexión clásica o una conexión inalámbrica según la configuración.

Como se ha indicado anteriormente, según un modo de realización particular, la interfaz de comunicación 115, utilizada como concentrador entre la estación huésped, el controlador de memoria y el microcontrolador protegido, es sustituida por dos interfaces de comunicación distintas, estando conectados cada uno del microcontrolador protegido y del controlador de memoria a una de estas interfaces conectable por otro lado cada una de ellas a la estación huésped.

A título de ilustración, la entidad electrónica portátil según este modo de realización puede ser una tarjeta de microcircuitos de conformidad con la norma ISO 7816, que incluye un sello con ocho contactos de los que dos pueden conectarse al microcontrolador protegido. Por otro lado, de manera estándar, otros dos contactos se dedican a los intercambios de datos de acuerdo con la norma USB. Los dos contactos USB se unen exclusivamente al controlador de memoria y permiten a este comunicar con una estación huésped. Los contactos de alimentación y de reloj están compartidos con los de la norma ISO 7816.

La figura 2 ilustra un ordenador 200 al que puede conectarse la llave USB 100 ilustrada en la figura 1. El ordenador 200 comprende en este caso una unidad central 205 de la que se ilustra un ejemplo de arquitectura en la figura 6, una pantalla 210, un teclado y un dispositivo puntero 215. La unidad central 205 comprende una interfaz de comunicación 220, en este caso un conector USB, adaptado para recibir la llave USB 100.

La unidad central 205 comprende un módulo de software de comunicación de datos para recibir y transmitir unos datos a través de la interfaz de comunicación 200. Un módulo de software de comunicación de ese tipo es denominado también *driver* en terminología anglosajona.

La unidad central 205 está adaptada además para ejecutar un software de control que permita principalmente recibir, a través de otra aplicación o a través de los medios de entrada, y transmitir, a través de la interfaz de comunicación 220, unos datos de autentificación tales como una firma o una contraseña.

El software de control está adaptado igualmente para transferir datos a cifrar hacia la llave USB 100 y para recibir datos descifrados de esta y recíprocamente.

Según un modo de realización particular, el software de control ejecutado por la unidad central 205 es recibido por la llave USB 100 cuando esta está conectada. El software de control puede borrarse automáticamente o no de la estación huésped con la desconexión de la llave USB 100.

La figura 3 ilustra un ejemplo de algoritmo implementado en la estación huésped, después de la conexión de una entidad electrónica portátil de acuerdo con la invención, que permite acceder a unos datos cifrados en o a través de una entidad electrónica portátil de ese tipo.

De ese modo, como se ha ilustrado, después de la conexión de la entidad electrónica portátil (etapa 300), se ejecuta el software de control (etapa 305).

El software de control, comprendiendo en este caso las etapas 310 a 340, se memoriza preferentemente en la memoria 105 de la entidad electrónica portátil. Después de la transmisión de este desde la entidad electrónica portátil a la estación huésped, se ejecuta según un comando de ejecución automática, denominado *autorun* en terminología anglosajona. La ejecución automática puede implementarse, por ejemplo, creando una subinterfaz de tipo lector de CD-ROM, de acuerdo con la norma USB.

Alternativamente, esta aplicación puede estar presente en la estación huésped. Puede ejecutarse automáticamente durante la conexión de la llave USB 100 o ejecutarse por el usuario.

Después del lanzamiento del software de control, se invita al usuario a autentificarse (etapa 310) introduciendo, por ejemplo un código PIN con ayuda de los medios de entrada/salida de la estación huésped tales como un teclado. Alternativamente, pueden utilizarse otros tipos de datos para autentificar al usuario. A título de ilustración, estos datos pueden ser datos biométricos tales como una huella digital o una foto de identidad (estos datos pueden adquirirse a través de un captador correspondiente) o unos datos criptográficos tales como una firma que pueda memorizarse en una tarjeta de microcircuitos accesible a la estación huésped.

Estos datos autentificación se transmiten entonces a la entidad electrónica portátil (etapa 315) a través de la interfaz de comunicación que une la estación huésped a esta entidad. De manera ventajosa, los datos de autentificación se transmiten a la entidad electrónica portátil según el protocolo USB o un protocolo similar, en la forma de paquetes de datos, denominados APDU (siglas de *Application Protocol Data Unit* en terminología anglosajona).

De ese modo, de manera general, la aplicación de control de acceso lanzada en la estación huésped permite introducir o recibir datos de autentificación del usuario, siendo transmitidos estos datos a continuación a la entidad electrónica portátil.

La aplicación de control de acceso es preferentemente una aplicación que comprende una interfaz gráfica del tipo de las implementadas por el sistema operativo de la estación huésped.

En respuesta a los datos de autentificación, la entidad electrónica portátil transmite un mensaje indicando si el usuario está autentificado o no. Como se sugiere por la flecha en trazo de puntos, si el usuario no está autentificado, es invitado de nuevo a introducir unos datos de autentificación. De manera ventajosa, la entidad electrónica portátil se bloquea automáticamente después de varias tentativas infructuosas de autentificación, por ejemplo después de tres tentativas. Entonces, preferentemente, se detiene el software de control.

Alternativamente, los datos de autentificación son adquiridos directamente en la entidad electrónica portátil con ayuda de, por ejemplo, un captador biométrico tal como un captador de huellas digitales o de un teclado que permita introducir un código de acceso.

Si el usuario está autentificado, el software de control transmite a la entidad electrónica portátil una solicitud (etapa 320) para acceder a los datos cifrados memorizados en esta o accesibles a través de esta. Alternativamente, la solicitud puede no dirigirse más que a ciertos datos cifrados, particularmente a una partición o un archivo específico.

Según un modo de realización particular, los datos cifrados se memorizan en la forma de un archivo cifrado, siendo presentados estos datos, después del descifrado, en la forma de una partición.

La solicitud para acceder a los datos tiene en este caso por objeto la lectura del encabezado del archivo cifrado que representa los datos. Después de haberse recibido, este encabezado se transmite al microcontrolador protegido de la entidad electrónica portátil en el que se calcula una clave de descifrado Kd a partir del encabezado, de una clave maestra memorizada en el microcontrolador protegido y, ventajosamente, de al menos una parte de los datos de autentificación previamente recibidos.

Si la clave de descifrado es válida, se transmite un mensaje de acuse de recibo al software de control que recupera entonces el conjunto de los datos del archivo cifrado (etapa 235). Estos datos se memorizan, por ejemplo, en un archivo denominado Acifrado en la memoria de la estación huésped.

Los datos contenidos en este archivo se transmiten entonces a la entidad electrónica portátil (etapa 330), con destino en el microcontrolador protegido, en el que se descifran con ayuda de la clave Kd previamente determinada y se retransmiten con destino en la estación huésped.

Los datos descifrados recibidos por la estación huésped (etapa 335) se memorizan en esta, por ejemplo en la forma de un archivo llamado Aclaro.

Como se ilustra por la flecha en trazo de puntos, las etapas 330 y 335 se repiten mientras se hayan descifrado, por el microcontrolador de la entidad electrónica portátil, todos los datos del archivo cifrado (Acifrado) memorizado en la estación huésped.

De ese modo, el archivo Aclaro es la imagen, descifrada, del archivo Acifrado que es a su vez la copia de un archivo similar memorizado en la memoria en masa de la entidad electrónica portátil o en una memoria en masa a la que está conectada.

Se crea entonces una partición virtual, en la estación huésped, mediante el software de control a partir de los datos del archivo descifrado Aclaro (etapa 340). Esta partición virtual se ve, preferentemente, como un disco duro de la estación huésped.

El usuario puede acceder entonces a los datos de esta partición virtual, modificarlos, suprimirlos o añadir nuevos datos, tal como lo haría con otras particiones.

La figura 4 ilustra un ejemplo de algoritmo que puede ejecutarse por una entidad electrónica portátil de conformidad con la invención, después de la conexión de esta a una estación huésped, para permitir a esta última acceder a unos datos cifrados en o a través de esta entidad electrónica portátil.

Después de la conexión de la entidad electrónica portátil a una estación huésped (etapa 400) y después de haber recibido los datos de autentificación (etapa 405), por ejemplo un código PIN, se efectúa una prueba para autentificar al usuario a través de estos datos (etapa 410). Como se ha indicado anteriormente, los datos de autentificación pueden recibirse ya sea desde la estación huésped o ya sea desde un captador o desde medios de introducción directamente integrados en la entidad electrónica portátil.

La naturaleza de la prueba de autentificación depende de la naturaleza de los datos de autentificación recibidos. Si los datos recibidos son una contraseña, un código PIN o unos datos biométricos, por ejemplo unos datos representativos de una huella digital o de una foto de identidad, esta prueba puede consistir en comparar los datos recibidos con unos datos previamente memorizados, preferentemente, en una memoria de tipo EEPROM de la entidad electrónica portátil. El usuario es autentificado entonces si los datos son similares. Si los datos recibidos son unos datos criptográficos, se efectúa un cálculo para comparar la firma transportada por los datos con una clave secreta previamente registrada y memorizada, preferentemente, en una memoria de tipo EEPROM de la entidad electrónica portátil.

Si el usuario se ha autentificado, se transmite un mensaje de acuse de recibo a la estación huésped. En caso contrario, se transmite un mensaje para indicar que el usuario no está autentificado. Como se ha indicado anteriormente, el número de tentativas de autentificación está preferentemente limitado. Por ejemplo, después de tres tentativas de autentificación infructuosas, la entidad electrónica portátil se bloquea de tal manera que sea necesario esperar un tiempo predeterminado antes de poder autentificarse de nuevo y/o que sea necesario desconectar y reconectar la entidad electrónica portátil.

En esta fase, indicada por ①, los mensajes se intercambian entre la estación huésped y el microcontrolador protegido. No se recurre, en este caso, al controlador de memoria.

Cuando la entidad electrónica portátil recibe la solicitud de lectura de datos (etapa 415), se accede a los datos y se transmiten a la estación huésped (etapa 420). Es conveniente remarcar aquí que los datos se transmiten sin ser procesados. En consecuencia, si los datos están cifrados, se transmiten cifrados.

En esta fase, indicada por ②, los mensajes se intercambian entre la estación huésped y el controlador de memoria. No se recurre, en este caso, al microcontrolador protegido.

Cuando la entidad electrónica portátil recibe unos datos cifrados a descifrar (etapa 425), los datos se descifran (etapa 430), por ejemplo con ayuda de la clave Kd previamente determinada, y se retransmiten a la estación huésped (etapa 435).

En esta fase, indicada por ③, los mensajes se intercambian entre la estación huésped y el microcontrolador protegido. No se recurre, en este caso, al controlador de memoria.

Como se ha indicado anteriormente, el acceso a los datos de un archivo cifrado se realiza en varias etapas. Una primera etapa consiste en acceder al encabezado del archivo en la entidad electrónica portátil a través del

controlador de memoria y en retransmitirlo al microcontrolador protegido de la entidad electrónica portátil para determinar la clave de descifrado.

Los datos cifrados se leen a continuación en la entidad electrónica portátil a través del controlador de memoria y se retransmiten al microcontrolador protegido de la entidad electrónica portátil para ser descifrados.

De ese modo, no hay intercambio de datos entre el controlador de memoria y el microcontrolador protegido y, en consecuencia, no es necesario utilizar unos componentes o una arquitectura específica.

De manera similar, cuando debe desconectarse la entidad electrónica móvil, bajo solicitud del usuario o bajo solicitud de la estación huésped o de la entidad electrónica, los datos no cifrados accesibles en la partición creada en la estación huésped se cifran por la entidad electrónica portátil y posteriormente se transmiten y memorizan en esta o en una memoria en masa conectada a esta.

La figura 5 ilustra un ejemplo de algoritmo implementado en una estación huésped, en el software de control, para cifrar unos datos en una entidad electrónica portátil y memorizar estos datos en esta o a través de esta.

De ese modo, por ejemplo, cuando el usuario desea desconectar la entidad electrónica portátil o su solicitud de la estación huésped o de la entidad electrónica portátil, principalmente para efectuar un guardado de los datos, los datos presentes en la estación creada, que representan en este caso el archivo llamado Aclaro, se transmiten al microcontrolador protegido de la entidad electrónica (etapa 500) para ser cifrados ahí con ayuda de la clave Kd determinada durante el acceso a los datos. Si se trata de nuevos datos, se determina, por ejemplo, aleatoriamente una clave Kd.

Los datos cifrados recibidos en respuesta a esta solicitud de cifrado (etapa 505) se transfieren a continuación hacia el controlador de memoria de la entidad electrónica portátil (etapa 510) para ser ahí memorizados.

De manera ventajosa, los datos cifrados recibidos de la entidad electrónica portátil se memorizan en la estación huésped en la forma de un archivo cifrado (Acifrado) antes de ser transmitidos hacia la entidad electrónica portátil para ser ahí memorizados.

La figura 6 ilustra un ejemplo de algoritmo que puede ejecutarse por una entidad electrónica portátil según la invención para permitir a una estación huésped transferir unos datos en o a través de esta entidad electrónica portátil, estando memorizados estos datos en forma cifrada.

Antes de haber recibido unos datos no cifrados a cifrar (etapa 600), el microcontrolador protegido de la entidad electrónica portátil cifra los datos con la clave Kd correspondiente al usuario identificado y/o a los datos a cifrar (etapa 605) antes de retransmitirlos hacia la estación huésped (etapa 610).

Una parte de la clave Kd, llamada clave maestra se memoriza en el microcontrolador protegido, preferentemente en una memoria de tipo EEPROM, mientras que otra parte se asocia a los datos cifrados, preferentemente en forma de un encabezado.

En esta fase, indicada por ④, los mensajes se intercambian entre la estación huésped y el microcontrolador protegido. No se recurre, en este caso, al controlador de memoria.

Cuando la entidad electrónica portátil recibe los datos cifrados a memorizar (etapa 615), estos se memorizan en la memoria en masa de la entidad electrónica portátil o en una memoria en masa conectada a esta (etapa 620).

En esta fase, indicada por ⑤, los mensajes se intercambian entre la estación huésped y el controlador de memoria. No se recurre, en este caso, al microcontrolador protegido.

Se ilustra en la figura 7 una unidad central 205 adaptada para implementar la invención. Como se ha indicado anteriormente, la unidad central 205 se compone, por ejemplo, de un microordenador, un teléfono móvil o un asistente personal.

La unidad central 205 incluye en este caso un bus de comunicación 705 al que se unen:

- una unidad de procesamiento o microprocesador 710 (CPU);
- una memoria no volátil 715 (ROM) que puede incluir el programa “Prog” de control de acceso así como los módulos de software necesarios para la transmisión de datos entre la unidad central 205 y un periférico conectado a ella;
- una memoria volátil o memoria caché 720 (RAM) que incluye unos registros adaptados para registrar unas variables y parámetros creados y modificados en el transcurso de la ejecución de los programas antes citados; y,

- una interfaz de comunicación 750 adaptada para transmitir y para recibir unos datos, en particular para transmitir y para recibir unos datos a un periférico conectado a la interfaz 220.

La unidad central 205 puede disponer igualmente:

- de una pantalla 210 que permite visualizar unos datos y/o servir de interfaz gráfica con el usuario que podrá interactuar con los programas según la invención, con ayuda del teclado y de un ratón 215 o de otro dispositivo de introducción y de puntero;
- de un disco duro 735 que puede incluir el programa “prog” y los módulos de software de transmisión de datos antes citados y unos datos procesados o a procesar; y,
- de un lector de tarjeta 740 adaptado para recibir una tarjeta 745, por ejemplo la tarjeta de microcircuitos que comprende unos datos criptográficos de autentificación.

El bus de comunicación permite la comunicación e interoperabilidad entre los diferentes elementos incluidos en la unidad central 205 o unidos a ella. La representación del bus no es limitativa y, particularmente, la unidad central es susceptible de comunicar instrucciones a cualquier elemento de la unidad central 205 directamente o por intermedio de otro elemento de esta.

El código ejecutable de los programas que permite a la unidad central 205 implementar los procesos según la invención, puede almacenarse, por ejemplo, en el disco duro 735 o en la memoria no volátil 715.

Según una variante, el código ejecutable de los programas, en particular del programa de control de acceso, puede recibirse, al menos parcialmente, por medio de la interfaz 750, para almacenarse de manera idéntica a la descrita anteriormente.

La unidad central de procesamiento 710 controla y dirige la ejecución de las instrucciones o porciones de código de software del o de los programas.

Es conveniente observar que los elementos de la unidad central 205 necesarios para la implementación de la invención pueden disponerse igualmente en la forma de un aparato programado. Este aparato contiene entonces el código del o de los programas informáticos, por ejemplo fijado en un circuito integrado de aplicación específica (ASIC).

Naturalmente, para satisfacer unas necesidades específicas, una persona experta en la materia de la invención podrá aplicar unas modificaciones en la descripción precedente.

REIVINDICACIONES

1. Procedimiento para acceder a al menos un dato cifrado previamente memorizado en una memoria en masa de una entidad electrónica portátil (100) o en una memoria en masa accesible a través de dicha entidad electrónica portátil, adaptada dicha entidad electrónica portátil para conectarse a una estación huésped (200), comprendiendo dicha entidad electrónica portátil (100) unos medios de acceso (110) a dicha memoria en masa que comprende dicho al menos un dato cifrado y unos medios de protección (125) adaptados para descifrar dicho al menos un dato cifrado, siendo distintos e independientes dichos medios de acceso y dichos medios de protección y no intercambiando datos entre ellos, comprendiendo este procedimiento las siguientes etapas,

- recepción de dicho al menos un dato cifrado de dichos medios de acceso;
- transmisión de dicho al menos un dato cifrado recibido en dichos medios de protección para ser ahí descifrado; y,
- recepción de dicho al menos un dato descifrado,

implementándose dichas etapas en dicha estación huésped.

2. Procedimiento según la reivindicación anterior que comprende además una etapa de creación de una partición, comprendiendo dicha partición al menos dicho al menos un dato descifrado recibido.

3. Procedimiento según la reivindicación 1 o la reivindicación 2 que comprende además las siguientes etapas,

- transmisión de al menos una información de autentificación a dichos medios de protección; y,
- recepción de una indicación de autentificación,

implementándose dichas etapas en dicha estación huésped.

4. Procedimiento según la reivindicación anterior según el que dicho al menos un dato descifrado no se recibe más que después de la autentificación.

5. Procedimiento según la reivindicación 3, dependiente de la reivindicación 2, según el que dicha etapa de creación de partición no se realiza más que después de la autentificación.

6. Procedimiento para memorizar al menos un dato de manera cifrada en una memoria en masa de una entidad electrónica portátil (100) o en una memoria en masa accesible a través de dicha entidad electrónica portátil, estando adaptada dicha entidad electrónica portátil para conectarse a una estación huésped (200), y comprendiendo dicha entidad electrónica portátil (100) unos medios de acceso (110) a dicha memoria en masa y unos medios de protección (125) adaptados para cifrar dicho al menos un dato, siendo distintos e independientes dichos medios de acceso y dichos medios de protección y no intercambiando datos entre ellos, comprendiendo este procedimiento las siguientes etapas,

- transmisión de dicho al menos un dato a dichos medios de protección para ser ahí cifrado;
- recepción de dicho al menos un dato cifrado desde dichos medios de protección; y,
- transmisión de dicho al menos un dato cifrado a dichos medios de acceso para memorizar dicho al menos un dato cifrado en dicha memoria en masa,

implementándose dichas etapas en dicha estación huésped.

7. Procedimiento según una cualquiera de las reivindicaciones 2 a 5, siendo dependientes las reivindicaciones 3 a 5 de la reivindicación 2, que comprende además una etapa de memorización de todos los datos de dicha partición creada según el procedimiento de la reivindicación 6.

8. Procedimiento según la reivindicación anterior según el que dicha etapa de memorización de todos los datos se efectúa automáticamente en el transcurso de un procedimiento de desconexión de dicha entidad electrónica portátil.

9. Procedimiento según la reivindicación 7 según el que dicha etapa de memorización de todos los datos se efectúa bajo petición del usuario de dicha entidad electrónica portátil o de dicha estación huésped.

10. Procedimiento para acceder a al menos un dato cifrado previamente memorizado en una memoria en masa de una entidad electrónica portátil (100) o en una memoria en masa accesible a través de dicha entidad electrónica portátil, estando adaptada dicha entidad electrónica portátil para conectarse a una estación huésped (200), y comprendiendo dicha entidad electrónica portátil (100) unos medios de acceso (110) a dicha memoria en masa que comprende dicho al menos un dato cifrado y unos medios de protección (125) adaptados para descifrar dicho al menos un dato, siendo distintos e independientes dichos medios de acceso y dichos medios de protección y no intercambiando datos entre ellos, comprendiendo este procedimiento las siguientes etapas,

- recepción de una solicitud de acceso a dicho al menos un dato cifrado por dichos medios de acceso;
- transmisión de dicho al menos un dato cifrado a dicha estación huésped;
- recepción de dicho al menos un dato cifrado por dichos medios de protección;
- descifrado de dicho al menos un dato cifrado; y,
- transmisión de dicho al menos un dato descifrado a dicha estación huésped.

11. Procedimiento para memorizar al menos un dato de manera cifrada en una memoria en masa de una entidad electrónica portátil (100) o en una memoria en masa accesible a través de dicha entidad electrónica portátil, estando adaptada dicha entidad electrónica portátil para conectarse a una estación huésped (200), y comprendiendo dicha entidad electrónica portátil (100) unos medios de acceso (110) a dicha memoria en masa y unos medios de protección (125) adaptados para cifrar dicho al menos un dato, siendo distintos e independientes dichos medios de acceso y dichos medios de protección y no intercambiando datos entre ellos, comprendiendo este procedimiento las siguientes etapas,

- recepción de dicho al menos un dato por dichos medios de protección;
- cifrado de dicho al menos un dato en dichos medios de protección;
- transmisión de dicho al menos un dato cifrado a dicha estación huésped;
- recepción de dicho al menos un dato cifrado desde dicha estación huésped por dichos medios de acceso; y,
- transmisión de dicho al menos un dato cifrado a dicha memoria en masa para ser ahí memorizado.

12. Procedimiento según la reivindicación 10 o la reivindicación 11 que comprende además una etapa de recepción de al menos una información de autentificación y una etapa de autentificación del usuario de dicha entidad electrónica portátil.

13. Procedimiento según la reivindicación anterior según el que dicha etapa de autentificación se implementa en dichos medios de protección.

14. Procedimiento según la reivindicación 12 o la reivindicación 13 según el que dicha al menos una información de autentificación es recibida desde medios de introducción de dicha entidad electrónica portátil.

15. Procedimiento según una cualquiera de las reivindicaciones 12 a 14, dependientes de la reivindicación 10, según el que dichas etapas de descifrado y de transmisión de dicho al menos un dato descifrado no se ejecutan más que después de la autentificación de dicho usuario de dicha entidad electrónica portátil.

16. Procedimiento según una cualquiera de las reivindicaciones 12 a 14, dependientes de la reivindicación 11, según el que dichas etapas de cifrado y de transmisión de dicho al menos un dato cifrado no se ejecutan más que después de la autentificación de dicho usuario de dicha entidad electrónica portátil.

17. Dispositivo para entidad electrónica portátil (100) que comprende unos medios de acceso (110) a una zona de memoria y unos medios de protección (125), comprendiendo dichos medios de protección unos medios de cifrado y de descifrado adaptados para cifrar al menos un dato a memorizar en dicha zona de memoria y para descifrar dicho al menos un dato memorizado en dicha zona de memoria, estando adaptada dicha entidad electrónica portátil para conectarse a una estación huésped (200) y adaptada para realizar las etapas del procedimiento según una cualquiera de las reivindicaciones 10 a 16, dichos medios de acceso y dichos medios de protección son distintos e independientes y no intercambian datos entre ellos.

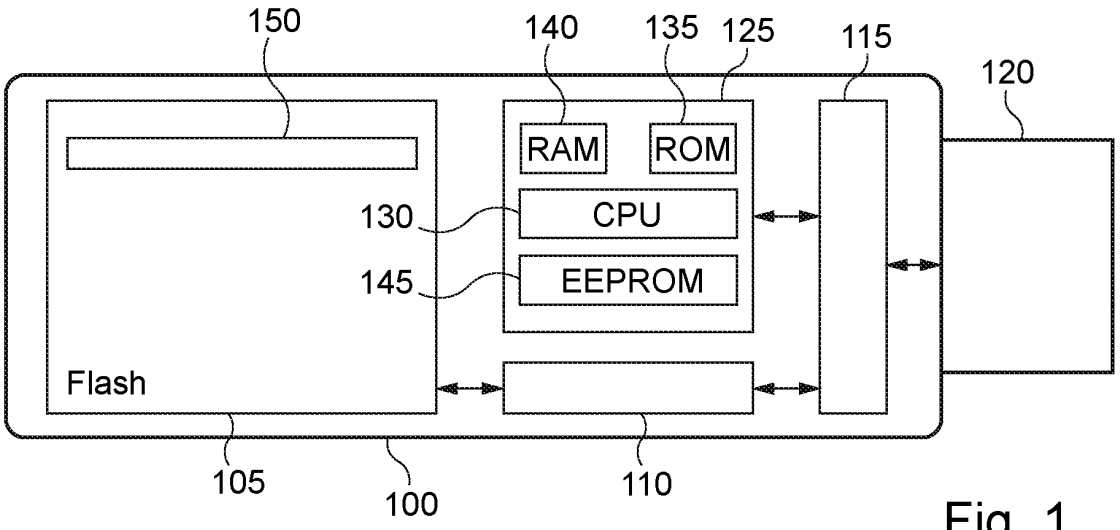
150
140
135
125
115
120
RAM
ROM
130
CPU
145
EEPROM
Flash
105
100
110

Fig. 1

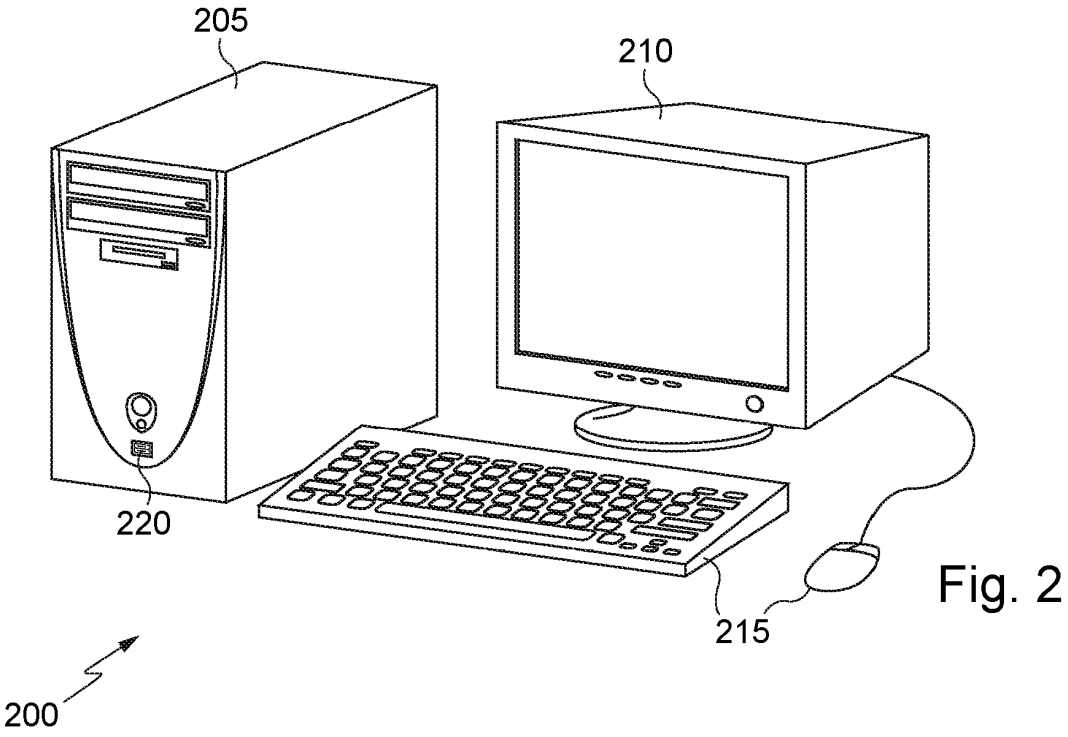
205
210
220
215
200

Fig. 2

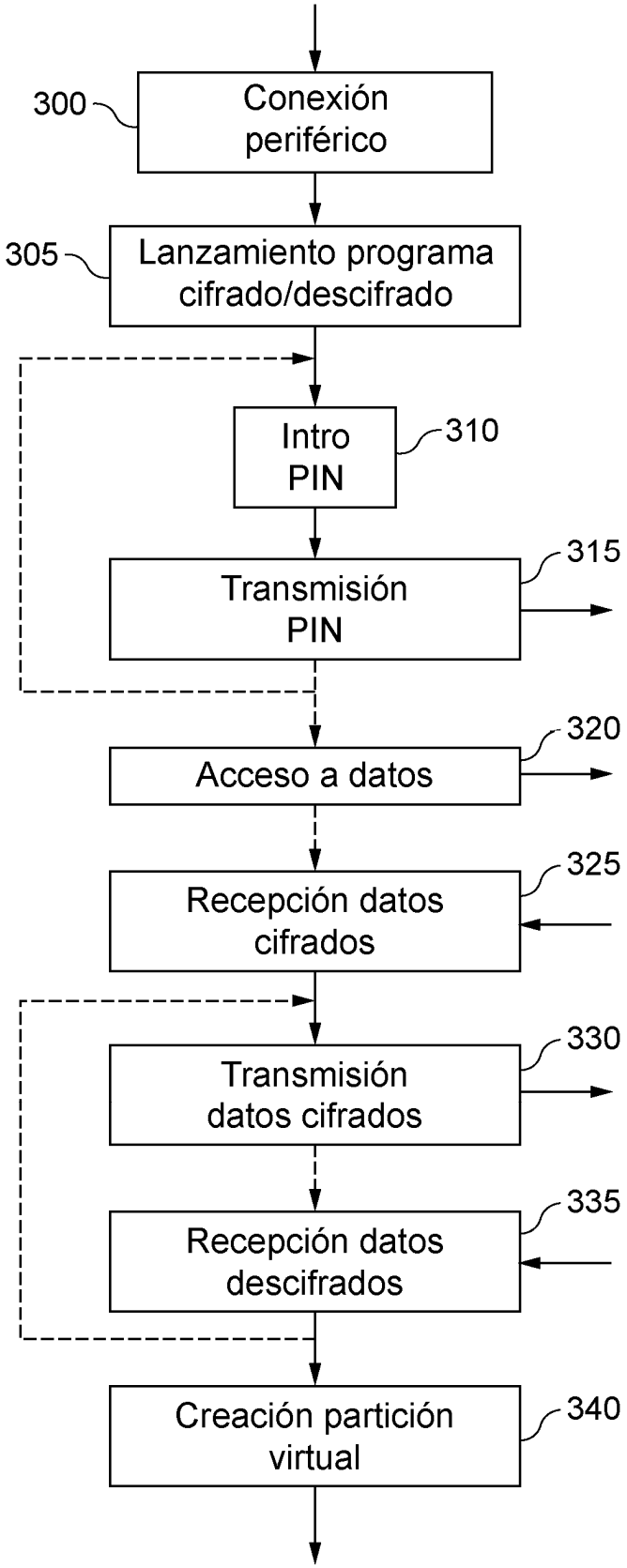
300
Conexión periférico
305
Lanzamiento programa cifrado/descifrado
Intro PIN
310
Transmisión PIN
315
Acceso a datos
320
Recepción datos cifrados
325
Transmisión datos cifrados
330
Recepción datos descifrados
335
Creación partición virtual
340

Fig. 3

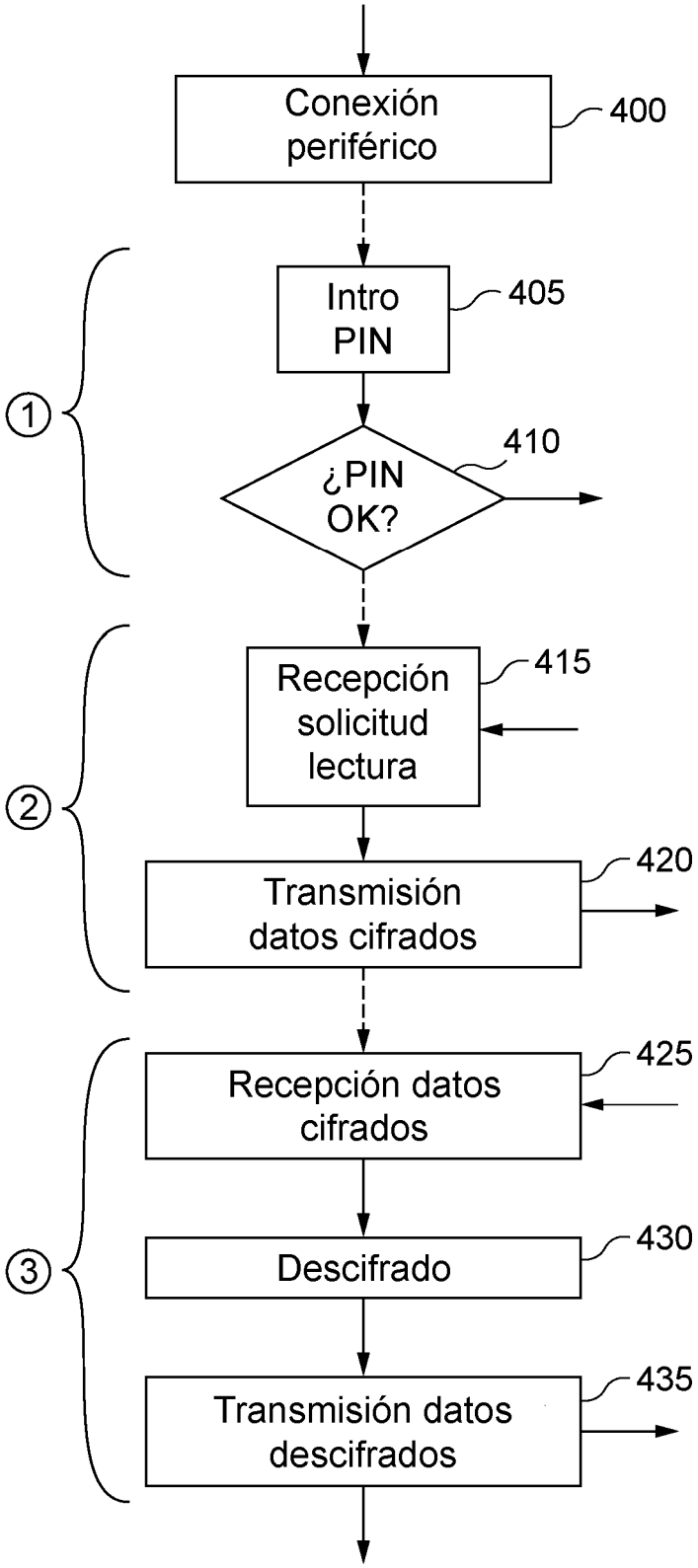
Conexión periférico
400
Intro PIN
405
¿PIN OK?
410
Recepción solicitud lectura
415
Transmisión datos cifrados
420
Recepción datos cifrados
425
Descifrado
430
Transmisión datos descifrados
435
1
2
3

Fig. 4

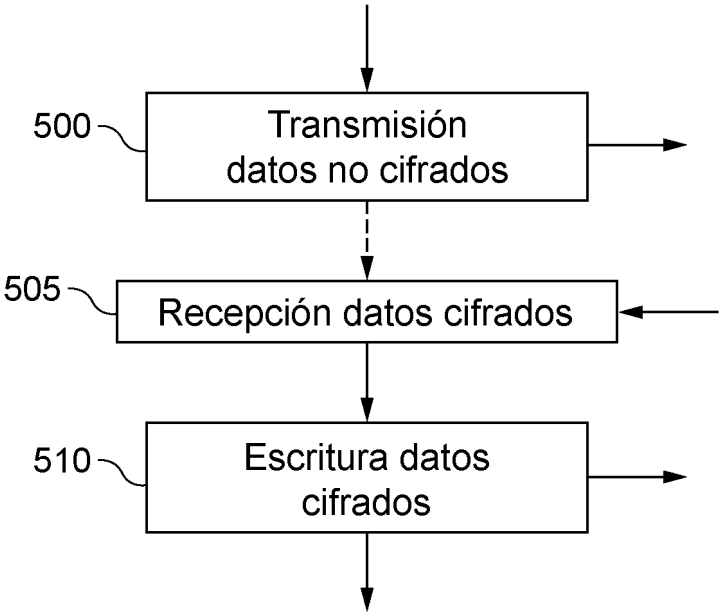
500
Transmisión datos no cifrados
505
Recepción datos cifrados
510
Escritura datos cifrados

Fig. 5

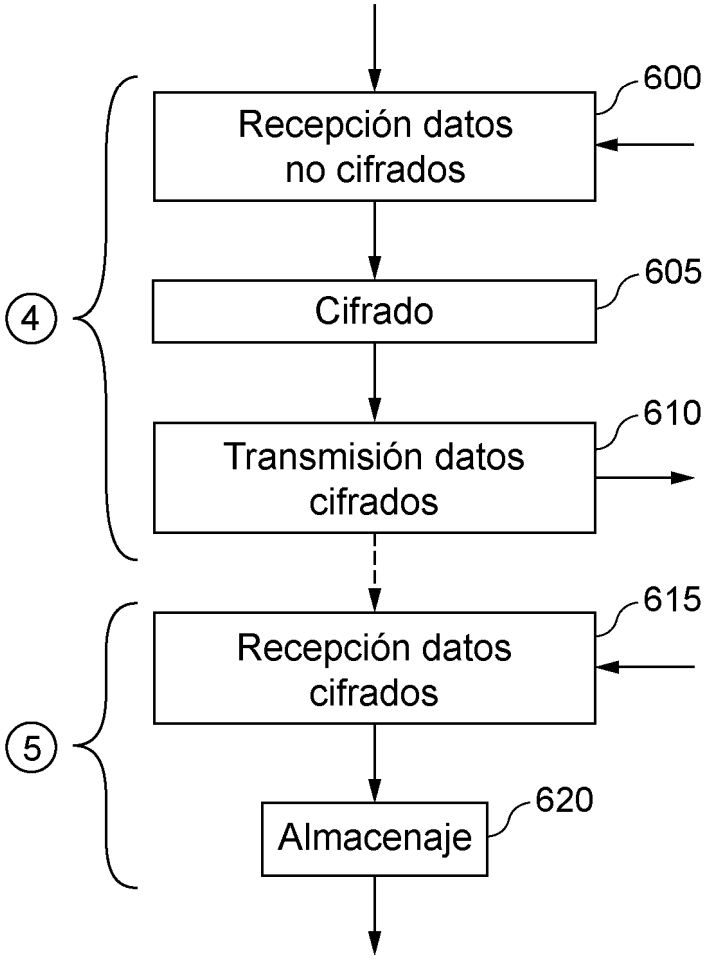
600
Recepción datos no cifrados
605
Cifrado
610
Transmisión datos cifrados
4
615
Recepción datos cifrados
5
620
Almacenaje

Fig. 6

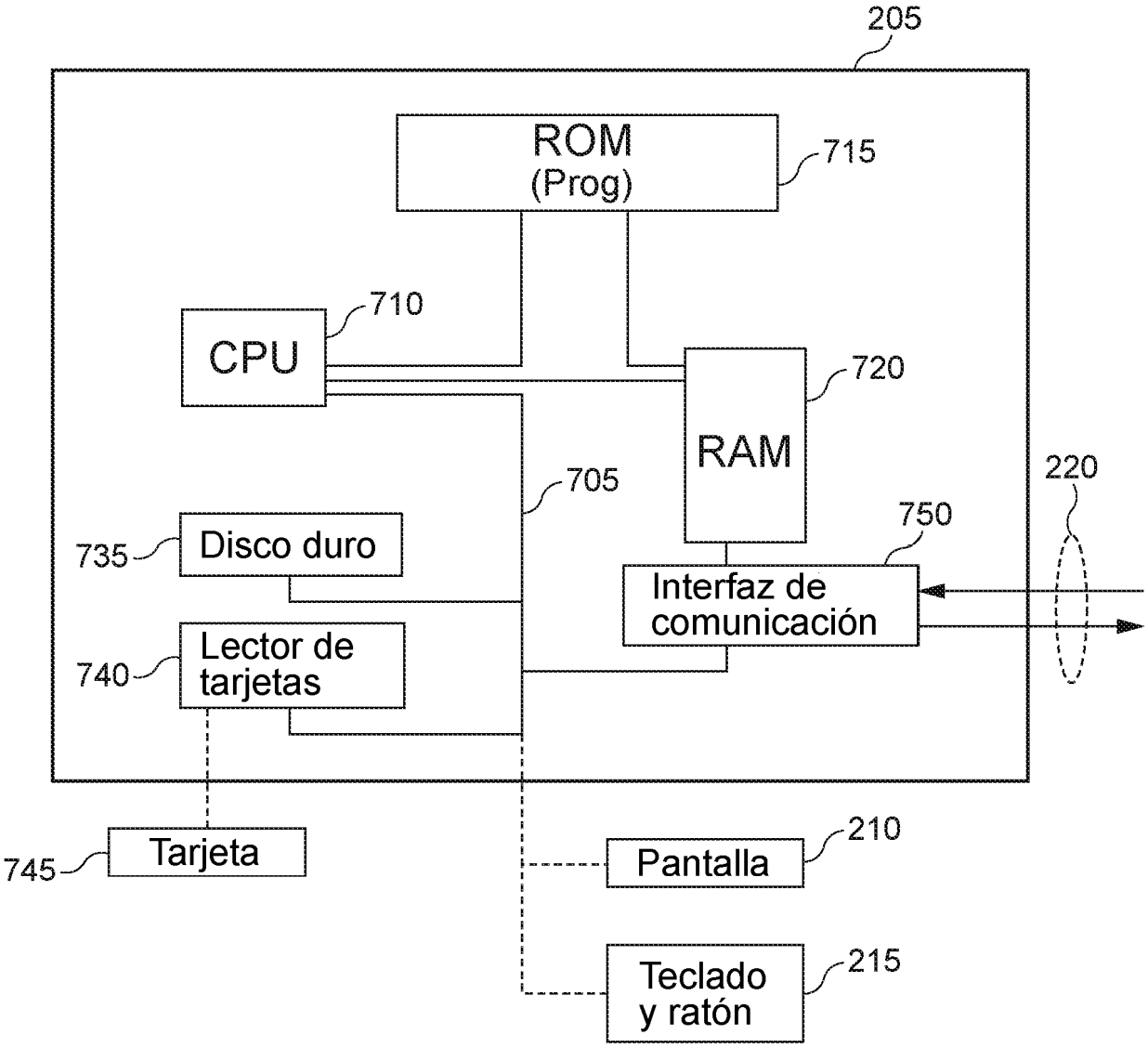
205
ROM
(Prog)
715
CPU
710
RAM
720
705
220
750
735
Disco duro
Interfaz de
comunicación
740
Lector de
tarjetas
745
Tarjeta
Pantalla
210
Teclado
y ratón
215

Fig. 7