(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 360 115**

(51) Int. Cl.:
***G07F 7/10*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05003236 .6**
(96) Fecha de presentación : **16.02.2005**
(97) Número de publicación de la solicitud: **1566776**
(97) Fecha de publicación de la solicitud: **24.08.2005**

(54) Título: **Procedimiento para el funcionamiento seguro de un soporte de datos portátil.**

(30) Prioridad: **19.02.2004 DE 10 2004 008 179**

(45) Fecha de publicación de la mención BOPI:
**01.06.2011**

(45) Fecha de la publicación del folleto de la patente:
**01.06.2011**

(73) Titular/es: **GIESECKE & DEVRIENT GmbH**
**Prinzregentenstrasse 159**
**81677 München, DE**

(72) Inventor/es: **Baldischweiler, Michael;**
**Bockes, Markus;**
**Drexler, Hermann;**
**Kahl, Helmut;**
**Karch, Torsten;**
**Lamla, Michael;**
**Mamuzic, Nikola;**
**Seysen, Martin;**
**Vater, Harald y**
**Weicker, Sabine**

(74) Agente: **Durán Moya, Luis Alfonso**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).



Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

**DESCRIPCIÓN**

La presente invención se refiere a un procedimiento para el funcionamiento seguro de un soporte de datos portátil. Además, la invención se refiere a un soporte de datos portátil.

En muchos campos de aplicación de los soportes de datos portátiles tales como, por ejemplo, en sistemas de pagos o controles de acceso, etc. resulta de vital importancia para el sistema en cuestión que no se pueda manipular el estado del soporte de datos portátil y que se pueda evitar la captación de datos secretos existentes en el soporte de datos portátil. Modificaciones muy críticas del estado del soporte de datos portátil son, por ejemplo, la modificación de los derechos de acceso a archivos almacenados en la memoria de dicho soporte de datos portátil, o una modificación del resultado que el soporte de datos portátil ha detectado al examinar un valor introducido para un número secreto personal. Como datos secretos pueden estar dispuestos en el soporte de datos portátil, por ejemplo, un código secreto personal para resetear el soporte de datos portátil tras su bloqueo etc. Los ataques externos potenciales pueden tener como objetivo la temporización del soporte de datos portátil, o bien intentar alterar el soporte de datos portátil, por ejemplo, mediante exposición a la luz o la subida o bajada transitorias de la tensión de servicio u otras influencias físicas. Dado que no se puede evitar que un soporte de datos portátil entre en la zona de influencia física de un atacante, es importante realizar el soporte de datos portátil lo más resistente posible a los ataques externos.

Por el documento WO 02/45035 A2 se da a conocer un procedimiento para la verificación de la integridad de datos confidenciales en el tratamiento de datos en aparatos electrónicos. El procedimiento consiste en calcular simultáneamente un valor de la totalidad del control, mientras se procesan los datos confidenciales. Los datos confidenciales son repartidos en conjuntos de octetos y son procesados y verificados octeto por octeto. Un ejemplo para las aplicaciones del procedimiento comprende la transmisión de datos de una memoria EEPROM de una tarjeta Smartcard a su memoria RAM y la validación de un código secreto en la tarjeta.

El documento US 2003/0188170 A1 se refiere a un procedimiento que pretende evitar las manipulaciones de un código secreto en un dispositivo de procesamiento de datos tal como, por ejemplo, una tarjeta Smartcard, utilizando un código antepuesto. El procedimiento para la utilización de una funcionalidad de la tarjeta comprende, antes de la implementación de un código, la transmisión de una función a los medios de procesamiento y la transformación del código secreto en un código secreto transformado en la tarjeta. Para cada utilización de la tarjeta se ponen a disposición una transformación y una comparación del código secreto transformado con el código secreto transformado en la tarjeta.

El objetivo de la invención es, por lo tanto, diseñar el funcionamiento de un soporte de datos portátil de manera que ofrezca la máxima seguridad.

Este objetivo se consigue mediante el procedimiento con la combinación de características según la reivindicación 1.

El procedimiento de la invención se refiere al funcionamiento seguro de un soporte de datos portátil que presenta una memoria en la que están almacenadas al menos una unidad de datos e informaciones que regulan el acceso a la unidad de datos. En el marco del procedimiento de la invención sólo se admiten aquellos accesos a la unidad de datos que son compatibles con las informaciones de acceso para dicha unidad de datos. La particularidad del procedimiento de la invención consiste en el hecho de que antes de permitir el acceso a la unidad de datos se comprueba si las informaciones de acceso y/o el procesamiento de las informaciones de acceso para esta unidad de datos han sido manipulados.

La invención presenta la ventaja de que se pueden impedir accesos no autorizados a unidades de datos del soporte de datos portátil, incluso cuando este soporte de datos portátil está expuesto a interferencias. Debido a ello se puede evitar la captación de datos secretos de un soporte de datos portátil o, al menos, hacerlo extremadamente difícil.

Según una realización preferente de la invención, al crear una unidad de datos se aplica un valor de comprobación. Este valor de comprobación puede depender de las informaciones de acceso y de una magnitud que caracteriza la unidad de datos. El valor de comprobación puede depender especialmente de las informaciones de acceso y del contenido de una unidad de datos. De este modo se establece una interconexión entre las informaciones de acceso y el contenido de la unidad de datos a proteger, de manera que una manipulación de la información de acceso puede detectarse fácilmente. Preferentemente, el valor de comprobación constituye una suma de comprobación, ya que ésta se puede calcular rápidamente y con poco coste.

Además, con el procedimiento de la invención se puede proceder de tal manera que, antes de autorizar un acceso a la unidad de datos, se constituye un valor de comprobación que se compara con el valor de comprobación aplicado. La evaluación de los valores de comprobación puede

realizarse de tal manera que sólo se autorizará un acceso a la unidad de datos cuando el nuevo valor de comprobación coincide con el valor de comprobación aplicado.

Otra medida para la protección del soporte de datos portátil puede consistir en el hecho de que, antes de autorizar un acceso a la unidad de datos, las informaciones de acceso son evaluadas varias veces sucesivamente, pudiéndose prever que un acceso a la unidad de datos sólo se autorizará, cuando se obtiene un resultado positivo de cada evaluación de las informaciones de acceso. Mediante este modo de proceder se pueden neutralizar especialmente ataques cuyo objetivo es una manipulación del proceso de evaluación, dado que es mucho más difícil tener éxito con una manipulación múltiple que con una sola manipulación.

Según una variante del procedimiento, según la invención, antes de autorizar el acceso o durante el acceso a la unidad de datos se verifican los parámetros del acceso varias veces. Esto tiene la ventaja de que se pueden detectar intentos de manipulación con los que se intenta modificar los parámetros de acceso.

El procedimiento de la invención también puede estar diseñado de tal manera que se pueden llevar a cabo múltiples veces comparaciones relevantes para la seguridad. Debido a ello resulta mucho más difícil, en general, llevar a cabo intentos de manipulación en comparaciones de este tipo.

Muy ventajoso resulta que se elija al azar el momento en el que se lleva a cabo al menos una operación relevante para la seguridad. De este modo se puede neutralizar intentos de manipulación con medios muy sencillos, ya que al atacante le resultará mucho más difícil iniciar su ataque en el momento oportuno. Esta forma de proceder puede aplicarse especialmente en las evaluaciones de las informaciones de acceso, las comprobaciones de los parámetros de acceso y las comparaciones relevantes para la seguridad que se han mencionado anteriormente.

Asimismo se puede aumentar la seguridad durante el funcionamiento del soporte de datos portátil borrando todos los datos secretos tras su uso en una memoria de trabajo del soporte de datos portátil que sirve para el almacenamiento temporal de datos.

El soporte de datos portátil de la invención presenta una memoria en la que se almacenan al menos una unidad de datos y las informaciones de acceso que regulan el acceso a dicha unidad de datos. Asimismo se prevé una función de seguridad que sólo autoriza accesos a la unidad de datos, cuando son compatibles con las informaciones de acceso para esta unidad de datos. La particularidad del soporte de datos portátil, según la invención, consiste en el hecho de que, cuando se produce un acceso a la unidad de datos, la función de seguridad comprobará si las informaciones de acceso para esta unidad de datos han sido manipuladas.

El soporte de datos portátil puede presentar, en especial, una memoria permanente cuyas áreas no utilizadas se llenan con instrucciones durante cuya ejecución no se llevan a cabo acciones algunas. Al final de las áreas no utilizadas puede estar almacenada una orden de salto, pudiendo la dirección de salto de la orden de salto estar situada dentro de la correspondiente área no utilizada. Asimismo, también es posible que la dirección de salto de la orden de salto señale una rutina que borra los datos a proteger de la memoria. Después del borrado, la rutina puede permanecer en un bucle sin fin. Mediante estas medidas se pueden evitar efectos nocivos producidos por saltos no definidos en la memoria permanente que pueden ser provocados, por ejemplo, por interferencias externas.

A continuación, se explicará la invención haciendo referencia a los ejemplos de realización mostrados en los dibujos.

Éstos muestran:

Figura 1: Un diagrama de bloques muy simplificado para un ejemplo de realización de un soporte de datos portátil;

Figura 2: Un ejemplo de realización para la estructura de un archivo aplicado en la memoria de un soporte de datos portátil; y

Figura 3: Un diagrama de flujo para una posible variante del desarrollo, según la invención, de un acceso de lectura al archivo.

En la figura 1 se muestra un diagrama de bloques muy simplificado para un ejemplo de realización de un soporte de datos portátil -1- en el que se puede aplicar el procedimiento, según la invención. Este soporte de datos portátil -1- puede ser, por ejemplo, una tarjeta con chip. El soporte de datos portátil -1- presenta una unidad de control -2- que controla las secuencias funcionales del soporte de datos portátil -1-. Asimismo, el soporte de datos portátil -1- presenta una unidad de entrada/salida -3- y una memoria -4-. En el ejemplo de realización mostrado la memoria -4- consta de una memoria permanente -5-, una memoria no volátil -6- y una memoria volátil -7-. Alternativamente la estructura de la memoria -4- también puede ser diferente. La unidad de control -2- está conectada con una unidad de

entrada/salida -3-, la memoria permanente -5-, la memoria no volátil -6- y la memoria volátil -7-. La unidad de entrada/salida -3- sirve para la comunicación con equipos externos que puede llevarse a cabo entrando en contacto físico con el soporte de datos portátil -1- y/o sin contacto.

En la memoria permanente -5- están aplicados datos que se mantienen invariables durante toda la vida útil del soporte de datos portátil -1-. El término datos se utilizará en adelante de forma muy general en el sentido de cualquier información independiente de su contenido, y ello puede englobar, por ejemplo, programas, parámetros, datos personales, claves, etc. En especial, se almacena en la memoria permanente -5- el sistema operativo del soporte de datos portátil -1-, estando todas las áreas no utilizadas de la memoria permanente -5- rellenadas con instrucciones que no provocan ningunas acciones. Al final de cada área no utilizada de la memoria permanente -5- está depositada una orden de salto cuya dirección de salto se ubica en la correspondiente área no utilizada de la memoria permanente -5-. Alternativamente, la dirección de salto de la orden de salto también puede señalar una rutina que borra los datos a proteger de la memoria -4-. Tras el borrado la rutina puede permanecer en un bucle sin fin. Mediante estas medidas se puede evitar un funcionamiento deficiente debido a saltos no definidos del contador de programa que pueden ser provocados por interferencias externas. Los saltos no definidos del contador de programa conllevan, por ejemplo, el riesgo de que se provoque una salida del contenido de la memoria volátil -7- en un momento en el que haya datos secretos aplicados en la misma.

La memoria volátil -7- sirve como memoria de trabajo para la unidad de control -2- de manera que los datos secretos son almacenados transitoriamente en la memoria volátil -7-, por ejemplo, cuando se lleva a cabo cálculos. Ciertamente el contenido de la memoria sólo se mantiene en la memoria volátil -7- mientras el soporte de datos portátil -1- está conectado a la alimentación. No obstante, el tiempo de permanencia de los datos secretos en la memoria volátil -7- debería ser lo más breve posible, borrándose estos datos de la memoria volátil -7- inmediatamente después de su uso. De esta manera se puede reducir más todavía el riesgo que comportan los saltos no definidos.

La memoria no volátil -6- puede ser reescrita una y otra vez durante la vida útil del soporte de datos portátil -1-. El correspondiente contenido de la memoria se conservará incluso cuando el soporte de datos portátil -1- no está conectado a la alimentación. En la memoria no volátil -6- están aplicados, por ejemplo, complementos para el sistema operativo, programas de aplicación, claves, datos personales, etc.

Con el procedimiento, según la invención, se deberán impedir accesos no autorizados a los datos aplicados en la memoria -4- del soporte de datos portátil -1-. Los datos están aplicados en archivos cuya estructura se explicará, a continuación, haciendo referencia a la figura 2.

En la figura 2 se muestra un ejemplo de realización para la estructura de un archivo -8- aplicado en la memoria -4- del soporte de datos portátil -1-. El archivo -8- está formado por una cabecera -9- y un cuerpo -10-. En el cuerpo -10- están aplicados los datos útiles del archivo -8-. La cabecera -9- presenta una serie de campos que contienen informaciones acerca del archivo -8-. El campo -11-, por ejemplo, contiene un nombre para poder identificar el archivo -8-. Asimismo, el campo -12- contiene las condiciones de acceso que regulan el acceso al archivo -8-. A través de las condiciones de acceso se asegurará que sólo se realicen accesos autorizados a los datos útiles del cuerpo -10- del archivo. A tal efecto se evaluará por medio de las condiciones de acceso, si un intento de acceso está autorizado. Sólo si en la evaluación se determina que existe una autorización, se permitirá el acceso. De este modo, un acceso de lectura a los datos útiles del cuerpo -10- se puede limitar, por ejemplo, sólo a aquellos archivos -8- que no contienen datos secretos y, de esta manera, se impide el espionaje de los datos secretos. Sin embargo, esto sólo está asegurado durante el funcionamiento normal del soporte de datos portátil -1-.

Cuando medidas perturbadoras tales como, por ejemplo, una exposición intensiva a la luz o una bajada o subida transitoria de la tensión de servicio u otras interferencias provocan una modificación de las condiciones de acceso, o se manipula la comprobación de dichas condiciones de acceso, entonces existe el riesgo de que los datos secretos del cuerpo -10- del archivo sean leídos sin autorización y eventualmente utilizados de forma indebida. Para evitar esto, se prevé, en el marco de la invención, un campo -13- en la cabecera -9- del archivo que contiene una suma de comprobación de las condiciones de acceso y los datos útiles del cuerpo -10- del archivo. Con la ayuda de esta suma de comprobación se puede detectar, si las condiciones de acceso a comprobar para autorizar un acceso a los datos útiles del cuerpo -10- del archivo han sido realmente predeterminadas tal como existen actualmente para estos datos útiles, o si han sido manipuladas. Como esto se lleva a cabo en concreto, se explicará haciendo referencia a la figura 3.

En la figura 3 se muestra un diagrama de flujo para una posible variante del desarrollo, según la invención, de un acceso de lectura al archivo -8-. El modo de proceder descrito se puede aplicar de forma análoga también a otros tipos de acceso tales como, por ejemplo, un acceso de escritura, etc. El desarrollo del diagrama de flujo empieza con una fase S1 en la que se hace la petición de un acceso de lectura al archivo -8-. A la fase S1 le sigue la fase S2 en la que se detecta un valor actual para la suma de comprobación a través de las condiciones de acceso y los datos útiles del archivo -8-. A la fase S2 le

sigue la fase S3 en la que se pregunta si el valor actual para la suma de comprobación coincide con un valor que está introducido en el campo -13- de la cabecera -9- del archivo -8-. El valor en el campo -13- ha sido detectado al crear el archivo -8- o durante una modificación autorizada del archivo -8-, e introducido en la cabecera -9-. Si se detecta en la fase S3 que el valor actual no coincide con el valor introducido en el campo -13- de la cabecera –9- para la suma de comprobación, entonces los datos útiles del cuerpo -10- y/o las condiciones de acceso se habrán modificado desde la entrada del valor para la suma de comprobación en el campo -13- de la cabecera -9-. Esto significa que no existen condiciones de acceso válidas para los datos útiles actuales del cuerpo -10-. Dado que, por lo tanto, existe el peligro de que las condiciones de acceso hayan sido manipuladas, en este caso a la fase S3 le seguirá una fase S4 en la que el acceso al archivo -8- será denegado y, en su caso, se iniciarán otras medidas destinadas a proteger el soporte de datos portátil -1-. Ahí acaba la evolución del diagrama de flujo.

Sin embargo, si en la fase S3 se comprueba que el valor actual coincide con el valor de la suma de comprobación introducido en el campo -13- de la cabecera -9-, a la fase S3 le seguirá una fase S5. En esta fase S5 se evalúan las condiciones de acceso para comprobar si se trata de un intento de acceso autorizado. Si la comprobación determina que no se trata de un intento de acceso autorizado, después de la fase S5 se llevará a cabo la fase S4 y ahí acaba la evolución del diagrama de flujo. Según una variación del procedimiento, según la invención, también se podría llevar a cabo una fase dispuesta expresamente para este caso, en la que análogamente a la fase S4 el acceso al archivo -8- es denegado, pero se llevan a cabo otras medidas de protección que en la fase S4. Si la comprobación de la fase S5 determina, sin embargo, que el intento de acceso tiene autorización le seguirá una fase S6 en la que se concede el acceso al archivo -8-. Para el presente ejemplo de realización esto significa que se leen los datos útiles aplicados en el cuerpo -10- del archivo. Con la fase S6 acaba la evolución del diagrama de flujo.

Para facilitar el cálculo de la suma de comprobación, también se puede prever de formar dicha suma de comprobación sólo a través la cabecera -9-. En este caso será necesario, sin embargo, que en la cabecera -9- se depositen parámetros que caracterizan el archivo -8- para que una modificación del archivo -8- tenga efectos sobre la cabecera -9- y, por lo tanto, también sobre la suma de comprobación.

La forma de proceder descrita anteriormente constituye una protección eficaz contra un acceso no autorizado cuando se intenta manipular las condiciones de acceso depositadas en el campo -13- en la cabecera -9- del archivo -8-. Sin embargo, un intento de manipulación también puede tener como objetivo la realización de la evaluación de las condiciones de acceso. Se podría interferir de tal manera en la evaluación que se conceda el acceso aunque una evaluación correcta de las condiciones de acceso hubiera tenido como resultado la denegación de este acceso. No se puede evitar un ataque de este tipo por tener en cuenta la suma de comprobación, ya que este ataque no requiere de ninguna manipulación en las condiciones de acceso. Pero con medios relativamente sencillos se puede conseguir que este ataque sea mucho más difícil. A tal efecto sólo se necesita repetir al menos una vez más la evaluación de las condiciones de acceso. La probabilidad que un segundo intento de manipulación puede llevarse a cabo con éxito exactamente en el momento de la repetición de la evaluación es ínfima. Las expectativas de que un ataque tenga éxito podrán ser reducidas más todavía, si la repetición no se lleva a cabo en un momento fijo después de la evaluación antecedente, sino que este momento sea elegido aleatoriamente. Lo que resulta importante es que el desarrollo del programa se ramifica con cada evaluación individual y el programa sólo llegará a conceder el acceso, si todas las evaluaciones acaban efectivamente con un resultado positivo. Para conseguir tanto una protección contra la manipulación de las condiciones de acceso, como también contra la manipulación de la realización de la evaluación de estas condiciones de acceso, se pueden combinar el hecho de tener en cuenta la suma de comprobación y la realización múltiple de la evaluación.

Otro intento de manipulación podría tener como objetivo manipular los parámetros de un acceso de lectura autorizado de tal manera que se leen datos fuera del archivo seleccionado -8-. En especial, se pueden manipular valores “Offset” o de longitud de las instrucciones de lectura. También en este caso, una contramedida satisfactoria consiste en comprobar los correspondientes parámetros varias veces y/o elegir aleatoriamente el momento en el que se realiza la comprobación.

Una comprobación múltiple y/o su realización en un momento elegido aleatoriamente pueden aplicarse también para comparaciones relevantes para la seguridad tales como, por ejemplo, la comprobación de un número secreto u otras operaciones relevantes para la seguridad.

Otra medida para aumentar la seguridad del soporte de datos portátil -1-, en concreto para neutralizar “timing attacks” (ataques de medición de tiempo), consiste en el hecho de programar todos los cálculos en los que se utilizan datos secretos de tal manera que el tiempo de cálculo no proporcione información alguna sobre los datos secretos. Además, para el cálculo, por ejemplo, de las sumas de comprobación no se han de utilizar procedimientos orientados a bits, sino procedimientos basados en uno o varios bytes tales como, por ejemplo, códigos Reed-Solomon o Hamming.

**REIVINDICACIONES**

1. Procedimiento para el funcionamiento seguro de un soporte de datos portátil (1) que presenta una memoria (4) en la que están almacenadas al menos una unidad de datos (8) e informaciones que regulan el acceso a la unidad de datos (8), en el que sólo se admiten aquellos accesos a la unidad de datos (8) que son compatibles con las informaciones de acceso para dicha unidad de datos (8), en el que antes de permitir el acceso a la unidad de datos (8) se comprueba si las informaciones de acceso y/o el procesamiento de las informaciones de acceso para esta unidad de datos (8) han sido manipulados, siendo aplicado un valor de comprobación al crear la unidad de datos (8), caracterizado porque el valor de comprobación depende de las informaciones de acceso y de una magnitud que caracteriza la unidad de datos (8) y/o del contenido de la unidad de datos (8).

2. Procedimiento, según la reivindicación 1, caracterizado porque el valor de comprobación representa una suma de comprobación.

3. Procedimiento, según una de las reivindicaciones 1 a 2, caracterizado porque antes de permitir un acceso a la unidad de datos (8), se forma un nuevo valor de comprobación que es comparado con el valor de comprobación aplicado.

4. Procedimiento, según la reivindicación 3, caracterizado porque sólo se permite un acceso a la unidad de control (8), cuando el nuevo valor de comprobación coincide con el valor de comprobación aplicado.

5. Procedimiento, según una de las reivindicaciones anteriores, caracterizado porque antes de permitir un acceso a la unidad de datos (8) las informaciones de acceso son evaluadas varias veces sucesivamente.

6. Procedimiento, según la reivindicación 5, caracterizado porque un acceso a la unidad de datos (8) se permite sólo cuando cada una de las evaluaciones de las informaciones de acceso da un resultado positivo.

7. Procedimiento, según una de las reivindicaciones anteriores, caracterizado porque antes de permitir un acceso o durante el acceso a la unidad de datos (8), se comprueban varias veces los parámetros del acceso.

8. Procedimiento, según una de las reivindicaciones anteriores, caracterizado porque se realizan varias veces comparaciones relevantes para la seguridad.

9. Procedimiento, según una de las reivindicaciones anteriores, caracterizado porque para al menos una operación relevante para la seguridad se elige el momento de su realización de forma aleatoria.

10. Procedimiento, según una de las reivindicaciones anteriores, caracterizado porque el soporte de datos portátil (1) comprende una memoria de trabajo (7) para el almacenamiento temporal de datos y porque todos los datos secretos son borrados de la memoria de trabajo (7) después de su uso.

11. Soporte de datos portátil para la realización del procedimiento, según la reivindicación 1, que comprende una memoria (4), en la que están depositadas al menos una unidad de datos (8) e informaciones de acceso que regulan el acceso a la unidad de datos (8), estando dispuesta una función de seguridad que sólo permite accesos a la unidad de datos (8) que son compatibles con las informaciones de acceso para esta unidad de datos (8), comprobando está función de seguridad antes de permitir un acceso a la unidad de datos (8) cada vez, si las informaciones de acceso y/o el procesamiento de las informaciones de acceso para esta unidad de datos (8) han sido manipulados, depositando esta función de seguridad un valor de comprobación al crear la unidad de datos (8), caracterizado porque la función de seguridad comprueba la dependencia del valor de comprobación de las informaciones de acceso y de una magnitud que caracteriza la unidad de datos (8).

12. Soporte de datos portátil, según la reivindicación 11, caracterizado porque se prevé una memoria permanente (5) y porque todas las áreas no utilizadas de dicha memoria permanente (5) están rellenadas con instrucciones cuya ejecución no provoca ninguna acción, y porque al final de cada área no utilizada está almacenada una orden de salto.

13. Soporte de datos portátil, según la reivindicación 12, caracterizado porque la dirección de salto de la orden de salto está situada dentro de la correspondiente área no utilizada.

14. Soporte de datos portátil, según la reivindicación 12, caracterizado porque la dirección de salto de la orden de salto señala a una rutina que borra los datos a proteger de la memoria (4).

15. Soporte de datos portátil, según la reivindicación 14, caracterizado porque la rutina permanece después del borrado en un bucle sin fin.

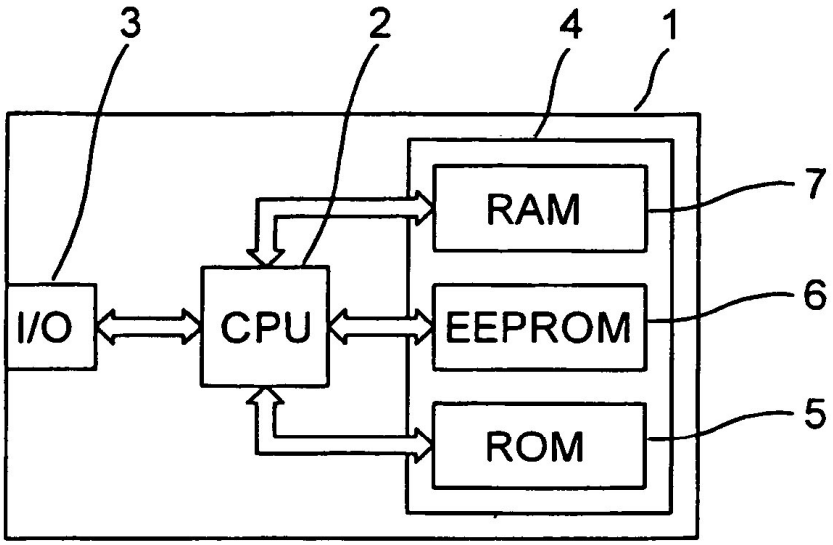


Fig. 1

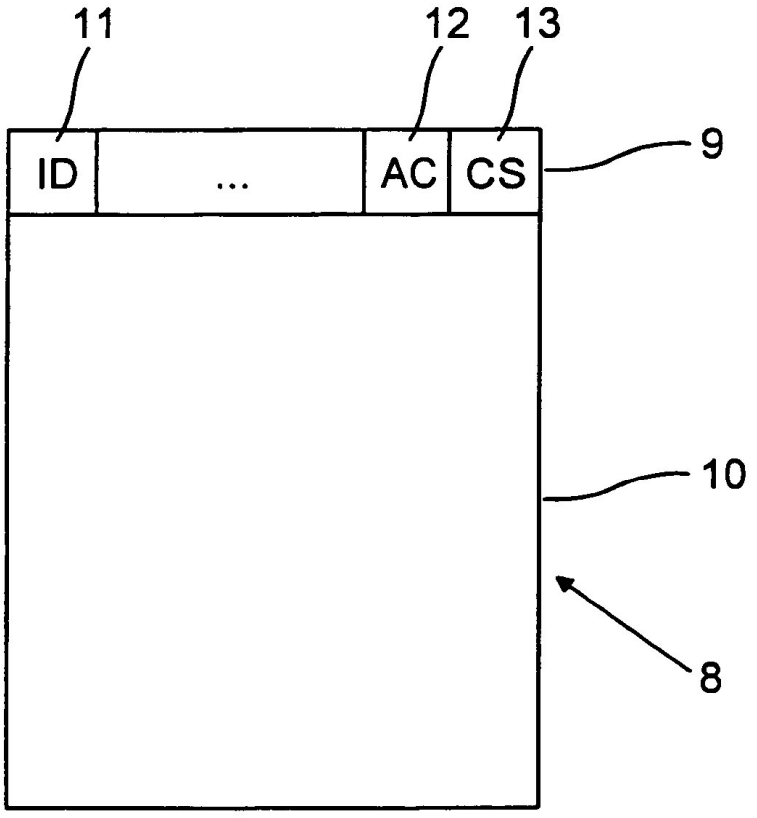


Fig. 2

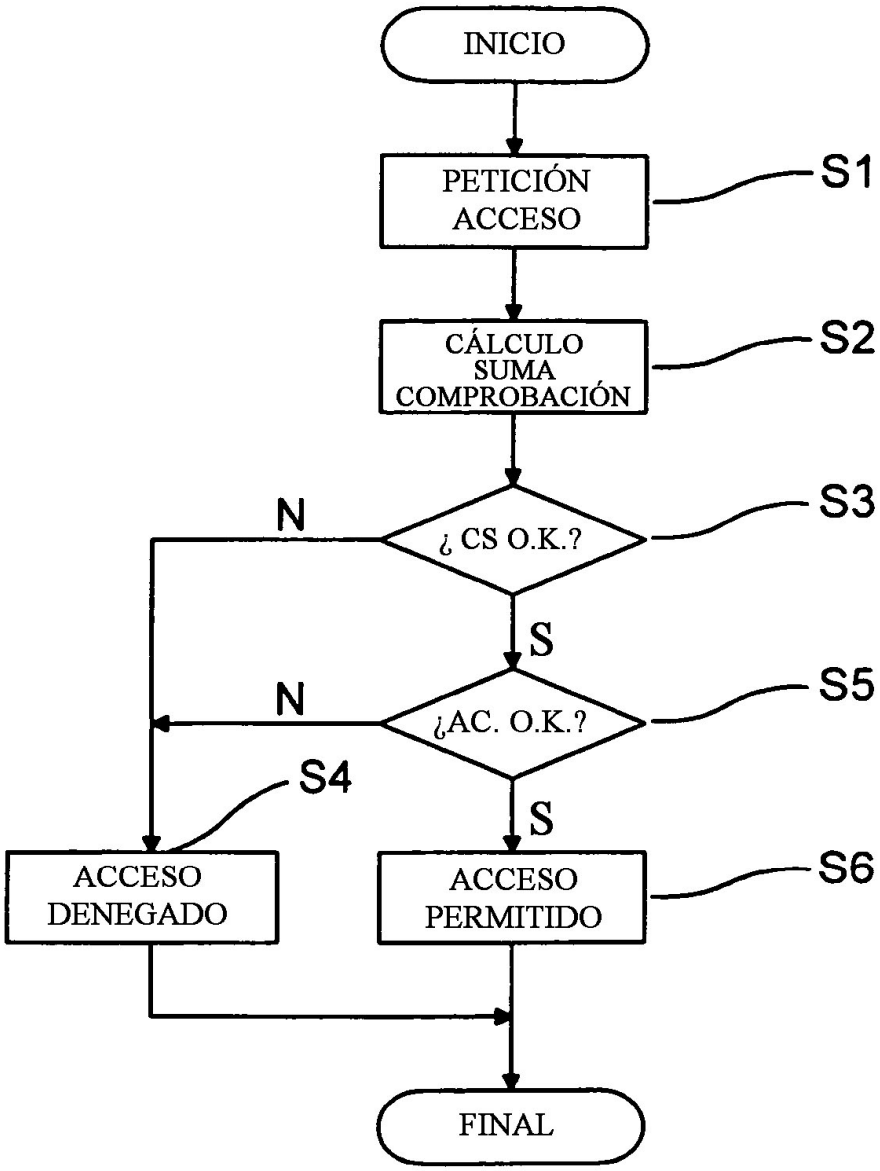
INICIO
PETICIÓN ACCESO
S1
CÁLCULO SUMA COMPROBACIÓN
S2
¿ CS O.K.?
S3
N
S
¿AC. O.K.?
S5
N
S
S4
ACCESO DENEGADO
ACCESO PERMITIDO
S6
FINAL

Fig. 3