(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 380 494**

(51) Int. CI.:
G07F 1/00 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07014168 .4**
(96) Fecha de presentación: **19.07.2007**
(97) Número de publicación de la solicitud: **1890269**
(97) Fecha de publicación de la solicitud: **20.02.2008**

(54) Título: **Puesta a disposición de una función de una ficha de seguridad**

(30) Prioridad:
10.08.2006 DE 102006037473

(45) Fecha de publicación de la mención BOPI:
14.05.2012

(45) Fecha de la publicación del folleto de la patente:
14.05.2012

(73) Titular/es:
GIESECKE & DEVRIENT GMBH
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:
Walter, Hinz y
Spitz, Stephan

(74) Agente/Representante:
Durán Moya, Luis Alfonso

DESCRIPCIÓN

Puesta a disposición de una función de una ficha de seguridad

La presente invención se refiere en general al ámbito de las fichas de seguridad y, más concretamente, al ámbito de la puesta a disposición de una función de una ficha de seguridad en un sistema de hospedaje. En los términos del presente documento, una ficha de seguridad puede ser, por ejemplo, una tarjeta con chip en diversas realizaciones, o bien un módulo con chip, por ejemplo en forma de conector USB. En los términos del presente documento, un sistema de hospedaje es, en general, cualquier dispositivo que aprovecha la función de la ficha de seguridad.

En dispositivos de telecomunicación móviles, por ejemplo teléfonos móviles, se utilizan generalmente tarjetas SIM ó USIM como ficha de seguridad. Estas tarjetas se encuentran de forma permanente dentro del dispositivo de telecomunicación y son alimentadas con energía eléctrica por el mismo durante todo el tiempo de funcionamiento del dispositivo de telecomunicación. Precisamente en dispositivos de telecomunicación compactos sería deseable poder aprovechar el espacio que ocupa la tarjeta también para otras cosas. Además, resulta deseable mantener el consumo eléctrico del dispositivo de telecomunicación lo más reducido posible. Existen problemas similares en otros sistemas de seguridad portátiles que utilizan tarjetas con chip u otras fichas de seguridad.

Otro campo de aplicación de fichas de seguridad son los sistemas de acceso condicional a datos de medios encriptados, por ejemplo decodificadores para programas de televisión de pago. Los sistemas de este tipo presentan a menudo múltiples ranuras para tarjetas con chip de diversos proveedores de programas de televisión de pago. Sin embargo, cada ranura genera costos, de manera que sería deseable poder ofrecer un gran confort para el usuario con una sola ranura.

Además, las fichas de seguridad se utilizan cada vez más para la autenticación de dos factores en aplicaciones críticas para la seguridad; el sistema de hospedaje es, en este caso, un ordenador habitual o bien un sistema embebido. También en este caso existe la necesidad de conseguir el mayor confort posible para el usuario con el menor coste posible.

En el documento US 2002/0080190 A1 se muestra un sistema para crear y gestionar “tarjetas con chip virtuales”. Un programa de control procede a la lectura de los datos contenidos en una tarjeta con chip física y los almacena, por ejemplo, en un disco duro o en un CD-ROM. Los datos almacenados pueden ser utilizados para la protección y el restablecimiento rápido de tarjetas con chip o pueden ser procesados mediante el programa de control. El programa de control puede, además, poner a disposición las funciones de la tarjeta con chip para programas de aplicación cuando la tarjeta con chip ha sido dañada o se ha perdido.

Por el documento WO 03/052565 A1 se conoce un dispositivo de ordenador que presenta una ficha de seguridad física y una zona de almacenamiento protegida con una ficha de seguridad virtual. La ficha física se utiliza para obtener el credencial (credential) para la ficha virtual.

Por el documento WO 2004/021715 A2 se da a conocer un procedimiento para poder utilizar una sola tarjeta SIM simultáneamente en un teléfono móvil y por un ordenador personal. La tarjeta SIM se halla en el teléfono móvil. Solicitudes dirigidas a la tarjeta SIM desde el ordenador son enviadas a través de una interfaz Bluetooth® al teléfono móvil y son contestadas allí por la tarjeta SIM. La respuesta es transmitida al ordenador a través de la interfaz Bluetooth.

En el documento US 2004/0072591 A1 se muestra un dispositivo para controlar el acceso a redes de telefonía móvil, en el que varias tarjetas SIM reales de diferentes proveedores están dispuestas en una unidad central. A tal efecto, los equipos de prueba envían solicitudes de autenticación a las tarjetas SIM y obtienen las respuestas generadas por las tarjetas SIM.

Por el documento US 2005/0227729 A1 se conoce un teléfono móvil que está destinado para ser utilizado por varios usuarios. Al teléfono móvil se puede conectar una tarjeta de memoria con datos personales tales como, por ejemplo, una agenda telefónica, datos de correo electrónico o datos de configuración. Cuando un usuario se da de alta en un teléfono móvil, los datos son transferidos de la tarjeta de memoria al teléfono móvil, y cuando el usuario se da de baja, los datos se vuelven a transferir otra vez a la tarjeta de memoria.

En el documento US 2002/0099634 A1 se muestra un sistema de transacciones con un servidor y varios terminales, cada uno de los cuales presenta múltiples unidades periféricas, en el que el servidor pone a disposición aplicaciones y controladores para las unidades periféricas.

En el documento US 2004/0117318 A1 se propone diseñar un soporte de datos portátil, de manera que un ordenador no puede iniciar la parte de confianza del ordenador sin el soporte de datos.

Un procedimiento para construir un canal seguro entre la tarjeta con chip y lectores de tarjeta está descrito en el documento US 2006/0085848 A1.

En el documento WO 01/93212 A2 se muestra una tarjeta con chip virtual en un ordenador, la cual comunica con el ordenador a través de la interfaz del lector de tarjeta, es decir que se maneja para aplicaciones igual que una tarjeta con chip físicamente presente.

En el documento WO 98/07092 A1 se prevé para un ordenador una unidad de seguridad adicional con lector de tarjeta y varias interfaces para ordenador, la cual lee los datos necesarios de varias tarjetas con chip para poder poner a disposición del ordenador de forma virtual las funciones de estas tarjetas con chip.

La invención tiene como objetivo poner a disposición una técnica que ofrece un alto grado de seguridad al tiempo que evita los problemas que se presentan al utilizar las fichas de seguridad, según el estado de la técnica. En algunas realizaciones, la invención contribuirá a poner a disposición dispositivos con un consumo eléctrico muy reducido y/o dispositivos muy económicos y/o dispositivos de manejo muy confortable.

De acuerdo con la invención, este objetivo se consigue totalmente o parcialmente mediante un procedimiento con las características indicadas en la reivindicación 1 y un sistema de hospedaje con las características indicadas en la reivindicación 12. Las reivindicaciones dependientes definen características opcionales de algunas realizaciones de la invención.

La invención parte de la idea básica de llevar a cabo un proceso de virtualización en el que se crea una ficha de seguridad virtual en una zona protegida del sistema de hospedaje, accediendo a una ficha de seguridad física. Una vez terminado el proceso de virtualización, la ficha de seguridad virtual pone a disposición, como mínimo, una función de la ficha de seguridad física. En la mayoría de las realizaciones ya no se necesitará más la ficha de seguridad física y ésta puede ser, por ejemplo, desconectada y/o retirada.

Debido a la utilización de un canal de comunicación protegido criptográficamente para la transmisión de datos y de una zona protegida para la creación de la ficha de seguridad virtual, mediante la invención se sientan las bases técnicas para proteger de forma fiable los datos secretos que están contenidos en la ficha de seguridad física, incluso durante la transmisión al sistema de hospedaje y durante la utilización de la ficha de seguridad virtual. Por lo tanto, la ficha de seguridad virtual también puede adoptar funciones críticas para la seguridad, por ejemplo, funciones de encriptado o desencriptado, o funciones de autenticación.

Por motivos de seguridad, en algunas realizaciones se ejecuta el proceso de virtualización cada vez que se carga el sistema de hospedaje para lo cual resulta imprescindible la ficha de seguridad física.

Mientras que en muchas realizaciones existe una relación 1:1 entre la ficha de seguridad física y la virtual, también se prevén otras realizaciones en las que se genera una sola ficha de seguridad virtual a partir de varias fichas de seguridad físicas, o se generan varias fichas de seguridad virtuales a partir de una sola ficha de seguridad física.

El sistema de hospedaje, según la invención, ha sido desarrollado en algunas realizaciones con características que corresponden a las características descritas anteriormente y/o que se indican en las reivindicaciones dependientes del procedimiento.

Otras características, ventajas y otros objetivos de la invención se desprenden de la siguiente descripción detallada de unos ejemplos de realización. Los dibujos esquemáticos muestran:

La figura 1 es un diagrama de bloques de un sistema de hospedaje y de una ficha de seguridad, según un ejemplo de realización de la invención;

La figura 2 es una representación de estructuras lógicas del ejemplo de realización mostrado en la figura 1, y

La figura 3 es un diagrama de flujo de un proceso de virtualización, según un ejemplo de realización de la invención.

En la representación esquemática de la figura 1 se muestran un procesador -12- y una memoria -14- con un sistema operativo -16- como componentes del sistema de hospedaje -10-. El sistema de hospedaje -10- puede ser, por ejemplo, un dispositivo portátil, por ejemplo, un dispositivo de telecomunicación portátil, o un ordenador convencional o un dispositivo embebido, por ejemplo, un sistema de acceso condicional. Se entiende que el sistema de hospedaje -10- presenta, en función de su realización exacta, otros componentes tales como, por ejemplo, una fuente de alimentación, un teclado y un indicador, los cuales no se muestran en la figura 1 para mayor claridad de representación.

El sistema de hospedaje -10- presenta, además, una interfaz -18- que está conectada con el sistema de hospedaje -10- a través de una ficha de seguridad -20-. La ficha de seguridad -20- es, por ejemplo, una tarjeta con chip o un módulo con chip. La interfaz -18- está adaptada a la ficha de seguridad -20-; la interfaz -18- puede estar realizada de acuerdo con una norma habitual para tarjetas con chip, por ejemplo, ISO/IEC 7816 ó GSM 11.11, o bien como interfaz USB o como interfaz para una tarjeta de memoria, por ejemplo, una tarjeta SD, MMC o SMMC. La ficha de

seguridad -20- contiene, de forma habitual, un procesador y una memoria con un sistema operativo, así como otros componentes; sin embargo, estos componentes no se muestran en la figura 1 para mayor claridad de representación.

El sistema operativo -16- del sistema de hospedaje -10- es un sistema operativo de seguridad apto para multitarea ("multitasking"), que permite la realización de procesos en el sistema de hospedaje -10-, cada uno en su propia zona, separadas una de la otra. Estas zonas se muestran en la figura 2 donde están señaladas con las referencias -22A-, -22B-, -22C- y en adelante se indicarán de forma conjunta como zonas -22x-. El sistema operativo -16- "particiona" o distribuye los recursos del sistema de hospedaje -10- en las zonas -22x-, por ejemplo, espacio de memoria en la memoria -14- y tiempo de ejecución del procesador -12-, de tal manera que las zonas -22x- están aisladas de forma segura las unas de las otras y tampoco es posible un acceso no autorizado desde el exterior a una de las zonas -22x-. Ello facilita el depósito y el procesamiento de datos críticos para la seguridad, por ejemplo, claves criptográficas en las zonas -22x-.

Tal como se muestra en la figura 2, durante el funcionamiento del sistema de hospedaje -10- un núcleo -24- del sistema operativo pone a disposición funciones básicas esenciales. Otras funciones del sistema operativo se llevan a cabo en, como mínimo, una zona reservada para servicios de sistemas operativos -26-, en este caso, por ejemplo en la zona -22A-. Según algunas realizaciones, el núcleo -24- del sistema operativo es un micronúcleo tal como, por ejemplo, el micronúcleo conocido con el nombre L4 que está descrito en el artículo "Toward Real Microkernels" (="Hacia los micronúcleos reales") de Jochen Liedtke, comunicaciones de ACM, vol. 39, nº 9, 1996, páginas 70-77. Un micronúcleo de este tipo puede conseguir un aislamiento muy seguro de procesos de sistemas operativos. Sin embargo, la invención no está limitada a sistemas operativos de micronúcleo.

La zona -22B- de la figura 2 sirve para la ejecución de un programa de aplicación -28- del sistema de hospedaje -10-. Se entiende que el sistema de hospedaje -10- puede presentar otros programas de aplicación, en la zona -22B, o en otras zonas.

En la zona -22C- se ejecuta un proceso de virtualización al iniciar el sistema de hospedaje -10- y cargar (boot) el sistema operativo -16- durante el cual se crea una ficha de seguridad virtual -30-. Para ello, resulta imprescindible la ficha de seguridad física -20-. Durante el proceso de virtualización se establece un canal de comunicación -32- protegido criptográficamente entre la ficha de seguridad física -20- y el proceso que crea la ficha de seguridad virtual -30-. Por ejemplo, puede tener lugar una autenticación mutua en cuyo transcurso se acuerdan los parámetros de seguridad para una comunicación encriptada, por ejemplo, una clave de sesión. Estos parámetros de seguridad los conoce sólo la ficha de seguridad física -20-, así como el proceso que crea la ficha de seguridad virtual -30-.

Dado que el canal de comunicación -32- protegido criptográficamente no es accesible ni para otros procesos en el sistema de hospedaje -10- ni tampoco para un atacante externo, todas las informaciones, incluidas las muy confidenciales, pueden ser transferidas de la ficha de seguridad física -20- a la ficha de seguridad virtual -30-. Debido a ello, es posible que la ficha de seguridad virtual -30- adopte todas las funciones de la ficha de seguridad física -20- durante el posterior funcionamiento. Por lo tanto, se produce una "virtualización completa de la ficha de seguridad".

Una vez terminado el proceso de virtualización, la ficha de seguridad física -20- ya no es necesaria. Puede ser desconectada y/o retirada. Debido a la desconexión de la ficha de seguridad física -20- se reduce el consumo eléctrico. Cuando se retira la ficha de seguridad física -20-, la interfaz -18- y/o el espacio ocupado por la ficha de seguridad -20- pueden ser aprovechados para otros fines.

La ficha de seguridad virtual -30- es implementada por un proceso que transcurre en la zona -22C- y accede a los datos almacenados asimismo en la zona -22C-. El sistema operativo -16- asegura en esta situación que la zona -22C- tiene a disposición una memoria fija y aislada, así como un cupo garantizado de tiempo de ejecución. La protección de memoria impide un acceso no autorizado de otros procesos a los datos de la ficha de seguridad virtual -30-, mientras que el cupo de tiempo de ejecución asegura la disponibilidad de la ficha de seguridad virtual -30- en el sistema de hospedaje -10-.

Al desconectar o cerrar el sistema de hospedaje -10-, según el presente ejemplo de realización, se borrará la ficha de seguridad virtual -30-, de manera que al iniciarlo la próxima vez se volverá a necesitar la ficha de seguridad física -20-.

Con el sistema descrito en la presente invención, se consigue en su conjunto una seguridad de fin a fin entre la ficha de seguridad física -20- y el sistema de hospedaje -10-. Dicho de otro modo, los datos que deben permanecer secretos sólo están presentes en texto plano dentro de la ficha de seguridad física -20- y dentro de la zona protegida -22C-. Dadas las altas exigencias en lo que se refiere a la seguridad del sistema operativo -16- y al aislamiento de la zona -22C-, el sistema de hospedaje -10- presenta, según algunas realizaciones, un TPM (Trusted Platform Module = módulo de plataforma segura) que sirve para proteger el sistema operativo -16-. Según otras realizaciones, es la ficha de seguridad física -20- que adopta la función del TPM mientras el mismo está conectado al sistema de hospedaje -10-. Pero también se prevén realizaciones en las que no se utiliza ningún hardware de protección

específico en el sistema de hospedaje -10-.

En la figura 3 se muestra la virtualización de la ficha de seguridad física -20- en un ejemplo de aplicación en el que la ficha de seguridad -20- es una tarjeta SIM ó USIM, y el sistema de hospedaje -10- es un teléfono móvil. En lo que se refiere a su forma de construcción, la ficha de seguridad -20- puede ser, por ejemplo, una tarjeta SMMC (Secure Multi-Media Card (Tarjeta Multimedia Segura)) y la interfaz -18- del sistema de hospedaje -10- está realizado de forma correspondiente como una ranura MMC. La representación de la figura 3 no está limitada a este ejemplo de aplicación que se acaba de indicar, sino que se aplica a muchas realizaciones de la invención. El sistema de hospedaje -10- puede ser, por ejemplo, un sistema de producción o un sistema de certificación o cualquier otro sistema que utiliza tarjetas con chip como fichas de seguridad físicas.

El proceso de virtualización que se muestra en la figura 3 se inicia al conectar y cargar el sistema de hospedaje -10-. En este momento, la ficha de seguridad física -20- ha de estar presente, es decir, en este ejemplo concreto la tarjeta SMMC ha de estar introducida en la ranura MMC del teléfono móvil. En realizaciones alternativas se pueden prever, de forma alternativa o adicional, otros sucesos iniciadores del proceso de virtualización.

En un proceso de construcción -34- se establece el canal de comunicación protegido -32- para lo cual se lleva a cabo, por ejemplo, una autenticación por desafío-respuesta con negociación de clave. A tal efecto se pueden utilizar procedimientos criptográficos en sí conocidos tales como, por ejemplo, procedimientos según los protocolos de mensajería segura (Secure Messaging) o SSL/TLS.

Los contenidos necesarios, por ejemplo claves y datos, de la ficha de seguridad física -20- son transferidos ahora en un proceso de transmisión -36- de la ficha de seguridad física -20- a la zona protegida -22C- del sistema de hospedaje -10-. Estos contenidos se utilizarán luego en un proceso de creación -38- para crear la ficha de seguridad virtual -30- en la zona -22C-. Según algunas realizaciones, el proceso de creación -38- puede llevarse a cabo una vez terminado el proceso de transmisión -36-. En general se solapan, sin embargo, el proceso de transmisión -36- y el proceso de creación -38-, total o parcialmente, y se llevan a cabo de forma paralela o entrelazada (interleaved), tal como se muestra en la figura 3.

Una vez inicializado la ficha de seguridad virtual -30- en el sistema de hospedaje -10-, se han terminado el proceso de creación -38- y, por lo tanto, todo el proceso de virtualización. El comportamiento de la ficha de seguridad física -20- es emulado ahora por la ficha de seguridad virtual -30-. Durante el subsiguiente funcionamiento del sistema de hospedaje -10-, todas las solicitudes que provienen, por ejemplo, del programa de aplicación -28- son dirigidas a la ficha de seguridad virtual -30- y respondidas por éste. La comunicación se realiza de acuerdo con las mismas normas que serían también pertinentes para la ficha de seguridad física -20- tales como, por ejemplo, las normas ESTI ó ISO/IEC-7816.

Ya no se necesita la ficha de seguridad física -20-. En el paso -40- es apagado, es decir, desconectado de la fuente de alimentación del sistema de hospedaje -10-. Ahora se puede retirar la ficha de seguridad física -20- de la interfaz -18-. De esta manera, en el presente ejemplo queda libre la ranura MMC del teléfono móvil. Esta ranura puede ser utilizada ahora, por ejemplo, para tarjetas MMC “normales”. Según algunas realizaciones, el sistema operativo -16- del sistema de hospedaje -10- puede decidir sobre otros posibles usos de la interfaz -18-. Por ejemplo, se puede prever que sólo se acepten tarjetas de memoria de un operador de sistema determinado.

Según el ejemplo que se acaba de describir, se ha convertido una sola ficha de seguridad física -20- en una sola ficha de seguridad virtual -30-. Sin embargo, esta asignación 1:1 no es obligatoria según algunas realizaciones. Por lo contrario, se prevén realizaciones en las que una ficha de seguridad virtual es creada a partir de varias fichas de seguridad físicas, y viceversa.

Un ejemplo de aplicación para la utilización de varias fichas de seguridad físicas -20- es un ente de certificación que expide, por ejemplo, certificados X.509. En un ente de certificación de este tipo, el sistema de hospedaje -10- puede ser una unidad de firma electrónica que trabaja con una “tarjeta con chip virtual” como ficha de seguridad virtual -30-. Según algunas realizaciones, se puede prever que para la creación de la ficha de seguridad virtual -30- se piden varias fichas de seguridad físicas -20- que pertenecen a diferentes usuarios. Mediante esta medida se consigue una muy alta seguridad total del ente de certificación.

Otro ejemplo de aplicación resulta de una ficha de seguridad física -20- que reúne varias funciones dentro del mismo. Una tarjeta con chip, por ejemplo, puede estar conformada tanto como una tarjeta SIM para servicios de comunicación móvil, como también como una tarjeta de desencriptado para la televisión digital. Debido al limitado paso de datos por la interfaz de la tarjeta con chip y/o debido a la limitada potencia de cálculo, puede resultar imposible utilizar estas funciones al mismo tiempo. Esto lo podrá remediar una virtualización si en el sistema de hospedaje -10- está disponible más potencia de cálculo para la ficha de seguridad virtual -30- y/o un mayor ancho de banda de comunicación entre la ficha de seguridad virtual -30- y los programas de aplicación, -28- por ejemplo. Según diferentes realizaciones, se puede convertir la ficha de seguridad física -20- en una sola ficha o en varias fichas de seguridad virtual -30-.

REIVINDICACIONES

1. Procedimiento para poner a disposición una función de una ficha de seguridad física (20) en un sistema de hospedaje (10), en el que se crea una ficha de seguridad virtual (30) en un proceso de virtualización (34, 36, 38) accediendo a la ficha de seguridad física (20), de manera que una vez terminado el proceso de virtualización (34, 36, 38), la ficha de seguridad virtual (30) proporciona la función que en sí proporciona la ficha de seguridad física (20) sin tener que recurrir a la ficha de seguridad física (20), caracterizado porque un sistema operativo del sistema de hospedaje (10) es un sistema operativo de seguridad apto para multitarea ("multitasking"), que permite que en el sistema de hospedaje (10) los procesos se realicen cada uno en su propia zona (22A, 22B, 22C), estando éstas separadas una de la otra, porque en la etapa de la creación de la ficha de seguridad virtual se transfieren datos que son necesarios para poner a disposición la función a través de un canal de comunicación criptográficamente protegido (32) de la ficha de seguridad física (20) al sistema de hospedaje (10) y porque la ficha de seguridad virtual (30) es creada en una zona (22C) del sistema de hospedaje (10) que es protegida por el sistema operativo.

2. Procedimiento, según la reivindicación 1, caracterizado porque el proceso de virtualización (34, 36, 38) se lleva a cabo, como mínimo, cada vez que se carga el sistema de hospedaje (10).

3. Procedimiento, según la reivindicación 1 ó 2, caracterizado porque la ficha de seguridad física (20) es desconectada una vez terminado el proceso de virtualización (34, 36, 38).

4. Procedimiento, según una de las reivindicaciones 1 a 3, caracterizado porque la ficha de seguridad física (20) puede ser separada del sistema de hospedaje (10) una vez terminado el proceso de virtualización (34, 36, 38).

5. Procedimiento, según una de las reivindicaciones 1 a 4, caracterizado porque la función que se pone a disposición es una función que requiere datos secretos para su ejecución, los cuales están contenidos en la ficha de seguridad física (20) y son transferidos al sistema de hospedaje (10) en el transcurso del proceso de virtualización (34, 36, 38).

6. Procedimiento, según una de las reivindicaciones 1 a 5, caracterizado porque la función que se pone a disposición es una función criptográfica, por ejemplo una función de encriptado o desencriptado, o una función de autenticación.

7. Procedimiento, según una de las reivindicaciones 1 a 6, caracterizado porque el proceso de virtualización (34, 36, 38) comprende un proceso de construcción (34) para establecer un canal de comunicación seguro (32), un proceso de transmisión (36) para transferir los datos requeridos para poner a disposición la función y un proceso de creación (38) para crear una ficha de seguridad virtual (30).

8. Procedimiento, según una de las reivindicaciones 1 a 7, caracterizado porque la ficha de seguridad física (20) es una tarjeta con chip o un módulo con chip.

9. Procedimiento, según una de las reivindicaciones 1 a 8, caracterizado porque la ficha de seguridad física (20) es una tarjeta SIM ó USIM, y porque el sistema de hospedaje (10) es un dispositivo de telecomunicación.

10. Procedimiento, según una de las reivindicaciones 1 a 9, caracterizado porque durante el proceso de virtualización (34, 36, 38) se crea la ficha de seguridad virtual (30) como única ficha de seguridad virtual (30) a partir de varias fichas de seguridad físicas entre las que se encuentra la ficha de seguridad física (20).

11. Procedimiento, según una de las reivindicaciones 1 a 9, caracterizado porque durante el proceso de virtualización (34, 36, 38) se crean varias fichas de seguridad virtuales entre las que se encuentra la ficha de seguridad virtual (30) a partir de la ficha de seguridad física (20), que constituye la única ficha de seguridad física (20).

12. Sistema de hospedaje (10) con un procesador (12) y una memoria (14) que está dispuesto para llevar a cabo todas las etapas de un procedimiento, según una de las reivindicaciones 1 a 11.

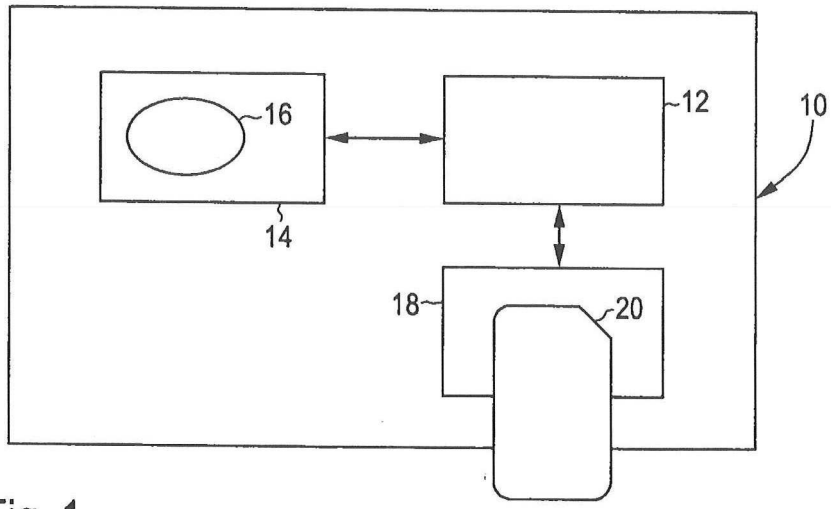

Fig. 1

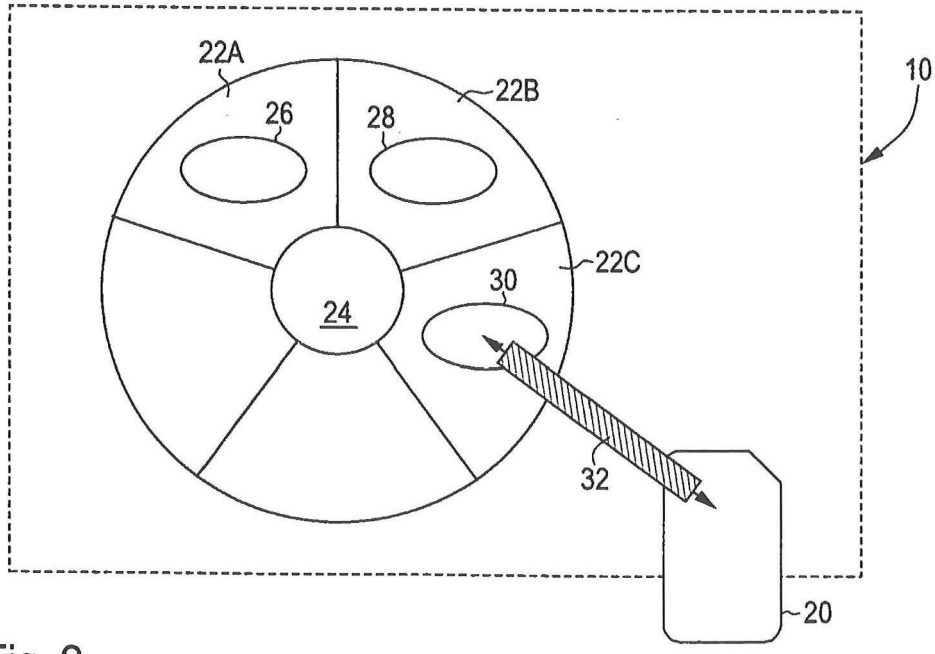

Fig. 2

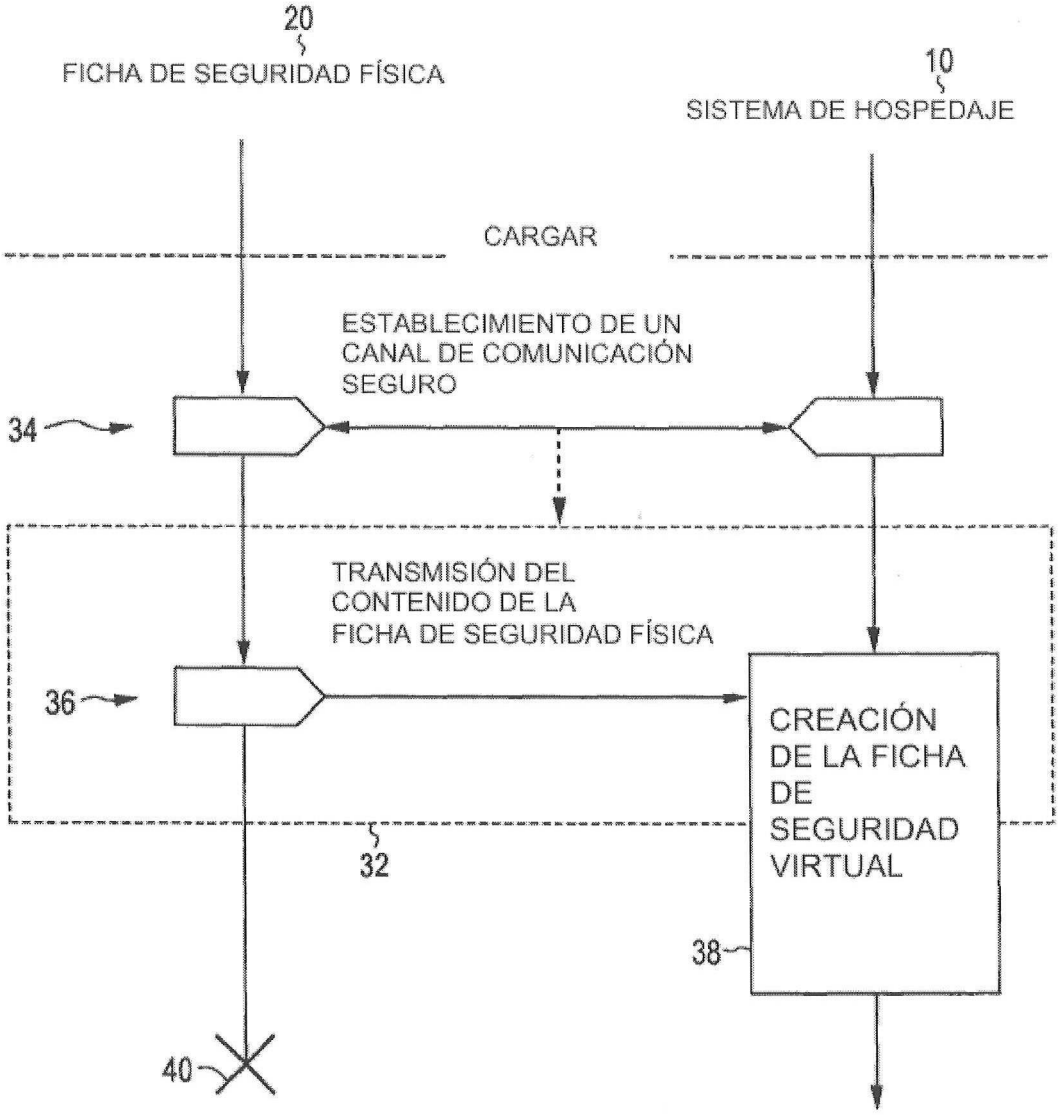
20
FICHA DE SEGURIDAD FÍSICA
10
SISTEMA DE HOSPEDAJE
CARGAR
ESTABLECIMIENTO DE UN CANAL DE COMUNICACIÓN SEGURO
34
TRANSMISIÓN DEL CONTENIDO DE LA FICHA DE SEGURIDAD FÍSICA
36
CREACIÓN DE LA FICHA DE SEGURIDAD VIRTUAL
32
38
40

Fig. 3