(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 643 223**

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.04.2010 PCT/EP2010/055518**

(87) Fecha y número de publicación internacional: **04.11.2010 WO10125021**

(96) Fecha de presentación y número de la solicitud europea: **26.04.2010 E 10717608 (3)**

(97) Fecha y número de publicación de la concesión europea: **02.08.2017 EP 2425368**

(54) Título: **Medio de almacenamiento con dispositivo de cifrado**

(30) Prioridad:

28.04.2009 DE 102009019051

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.11.2017

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

GROBBEL, HUBERTUS;
GUTER, FABIAN y
ROSIN, MARCUS

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Medio de almacenamiento con dispositivo de cifrado

La invención se refiere a un medio de almacenamiento con dispositivo de cifrado según el preámbulo de la reivindicación 1.

Un ejemplo de un medio de almacenamiento conocido en el sentido de la invención es una tarjeta de memoria Flash con opción de cifrado, con un criptoprocesador utilizado como dispositivo de cifrado y descifrado y una clave de cifrado y descifrado simétrica para cifrar datos, almacenada en la tarjeta. Con este tipo de tarjetas de memoria Flash, el usuario puede seleccionar de forma opcional a través de un menú de un terminal de tarjetas, por ejemplo, un ordenador con lector de tarjetas Flash conectado, o de un terminal de tarjetas móvil, como por ejemplo, un teléfono móvil con lector de tarjetas Flash, que los datos que se van a almacenar en la tarjeta de memoria Flash sean almacenados cifrados en la misma. Los datos almacenados sin cifrar pueden ser leídos de la tarjeta de memoria Flash. Los datos almacenados cifrados solo pueden ser leídos de la tarjeta de memoria Flash tras una autentificación exitosa del usuario con respecto a la tarjeta de memoria Flash. Si se intentan leer los datos almacenados cifrados sin autentificación, el proceso de lectura se cancela sin emisión de datos y, dado el caso, se emite un aviso de fallo o una solicitud de autentificación.

En algunos casos de aplicación, el poseedor de un medio de almacenamiento al que el propietario del medio de almacenamiento ha encargado el almacenamiento de datos en el medio de almacenamiento puede ser considerado por el propietario como potencialmente no fiable. Por ejemplo, un servicio de vigilancia que almacena fotografías o grabaciones de vídeo realizadas con fines de vigilancia en un medio de almacenamiento no debe tener la posibilidad de volver a leer las fotografías o grabaciones de vídeo ni de utilizarlas de forma inadecuada, por ejemplo, para fines privados en círculos de conocidos o para publicarlas en internet. Incluso aunque el medio de almacenamiento tenga una opción de cifrado, es posible que el poseedor no fiable simplemente no la utilice y por tanto pueda leer arbitrariamente los datos almacenados tras el almacenamiento.

El documento DE 198 03 218 A1 describe una tarjeta de memoria con algunas características del preámbulo de la reivindicación 1. Los datos deben cifrarse al ser introducidos en la tarjeta y descifrarse al ser leídos o bien introducirse y leerse sin cifrar. El documento US 2008/0071977 A1 muestra una tarjeta con sensor de huella dactilar, que se utiliza para permitir el acceso a los datos almacenados únicamente a usuarios autentificados.

El documento US 6.079.019 A describe una tarjeta de memoria IC con un canal de lectura de descifrado, a través del cual se pueden leer datos de forma descifrada en caso de una autentificación exitosa, y con un canal de lectura directo, mediante el cual se pueden emitir datos de forma cifrada en caso de una autentificación fallida.

El documento US 2007/113097 A1 da a conocer un medio de almacenamiento con dispositivo de cifrado según el preámbulo de la reivindicación 1. Los datos almacenados cifrados en una memoria del medio de almacenamiento son leídos de la memoria de forma descifrada en caso de una autentificación exitosa con respecto al medio de almacenamiento. En caso de una autentificación fallida se deniega el acceso a la memoria.

El objetivo de la invención consiste en crear un medio de almacenamiento con opción de cifrado que permita el almacenamiento seguro de datos, también en un entorno no fiable.

El objetivo se consigue mediante un medio de almacenamiento según la reivindicación 1. Las realizaciones preferentes de la invención se indican en las reivindicaciones dependientes.

El medio de almacenamiento está equipado con un área de memoria electrónica, una interfaz para introducir datos en el medio de almacenamiento y para leer datos del medio de almacenamiento, un dispositivo de introducción acoplado entre la interfaz y el área de almacenamiento para almacenar datos de la interfaz en el área de almacenamiento, un dispositivo de lectura acoplado entre la interfaz y el área de almacenamiento para emitir datos del área de almacenamiento a la interfaz, una memoria de clave en la que está almacenada o se puede almacenar una clave secreta, un dispositivo de cifrado acoplado al dispositivo de introducción para cifrar con la clave datos introducidos a la interfaz en el medio de almacenamiento y un dispositivo de descifrado acoplado al dispositivo de lectura para descifrar con la clave los datos emitidos del área de almacenamiento.

El medio de almacenamiento está caracterizado por que el dispositivo de introducción está configurado para cifrar todos los datos introducidos a la interfaz para su almacenamiento en el área de almacenamiento con la clave almacenada en la memoria de clave y almacenarlos cifrados en el área de almacenamiento, y por que el dispositivo de lectura presenta dos canales de lectura diferentes. Más precisamente existe un primer canal de lectura directo configurado para que, cuando se emiten datos mediante el canal de lectura directo, los datos almacenados cifrados en el área de almacenamiento puedan ser emitidos de forma cifrada a la interfaz evitando el dispositivo de descifrado. Además existe un segundo canal de lectura de descifrado configurado para que, cuando se emiten datos mediante el canal de lectura de descifrado, los datos almacenados cifrados en el área de almacenamiento puedan ser descifrados utilizando el dispositivo de descifrado con la clave almacenada en la memoria de clave, o una clave

de descifrado correspondiente a la clave y almacenada en la memoria de clave, y emitidos de forma descifrada a la interfaz.

Es decir que, por un lado, en este medio de almacenamiento todos los datos introducidos en la interfaz son cifrados sin posibilidad de acceso de un usuario del medio de almacenamiento. Esto permite encargar a personas no fiables el registro y almacenamiento de datos.

Además, los datos almacenados cifrados en el medio de almacenamiento se pueden emitir opcionalmente cifrados o descifrados. Por ejemplo, un empleado de un servicio de vigilancia que ha almacenado datos en el medio de almacenamiento puede leer los datos cifrados de forma cifrada del medio de almacenamiento y transferirlos de forma cifrada a una central fiable. Este procedimiento se puede aplicar, por ejemplo, en casos en que el empleado del servicio de vigilancia conserva el medio de almacenamiento y solo transfiere los datos a la central. En los casos en que la central no solo recibe los datos sino el medio de almacenamiento completo, un empleado fiable de la central puede descifrar los datos durante el proceso de lectura y emitirlos por tanto de forma descifrada desde el medio de almacenamiento.

Opcionalmente, el medio de almacenamiento también presenta un dispositivo de autentificación acoplado al dispositivo de lectura, que está configurado de forma que los datos puedan ser emitidos de forma descifrada a la interfaz mediante el canal de lectura como mucho en caso de una autentificación exitosa. De este modo se asegura que solo los usuarios fiables, caracterizados por que son capaces de autentificarse con respecto al medio de almacenamiento, pueden obtener los datos almacenados como texto legible, es decir, de forma descifrada o no cifrada.

Opcionalmente, el dispositivo de autentificación puede estar configurado además de forma que, en caso de una autentificación fallida, los datos sean emitidos mediante el canal de lectura directo de forma cifrada, es decir, tal como están almacenados en la memoria, es decir, igual que en el caso de una lectura sin autentificación.

Opcionalmente, el área de almacenamiento puede estar configurada además, al menos parcialmente, como memoria Flash. El medio de almacenamiento puede ser opcionalmente una tarjeta de memoria Flash configurada de forma inteligente, es decir, que presente un microprocesador de tarjeta inteligente y/o un criptoprocesador o similar.

Opcionalmente, como clave está prevista una clave simétrica de un sistema de cifrado simétrico. En este caso, para el cifrado y el descifrado se utiliza la misma clave. En principio también es posible utilizar para el cifrado y el descifrado dos claves diferentes y complementarias que opcionalmente pueden estar almacenadas ambas en el medio de almacenamiento, por ejemplo, en la memoria de clave.

El dispositivo de cifrado y el dispositivo de descifrado pueden estar configurados opcionalmente como dos dispositivos separados o como un único dispositivo de cifrado y descifrado combinado, y opcionalmente como uno o dos criptoprocesadores o microprocesadores de tarjeta inteligente.

A continuación se explica la invención en detalle en base a ejemplos de realización y haciendo referencia a los dibujos, que muestran:

La figura 1, un medio de almacenamiento según un modo de realización de la invención;
La figura 2, una introducción de datos en el medio de almacenamiento de la figura 1;
La figura 3, una lectura de datos del medio de almacenamiento de la figura 1 a través de un primer canal de lectura directo -A-;
La figura 4, una lectura de datos del medio de almacenamiento de la figura 1 a través de un segundo canal de lectura de descifrado -B-;
La figura 5, un descifrado posterior de datos leídos cifrados según la figura 3.

La figura 1 muestra un medio de almacenamiento -10- según un modo de realización de la invención con un área de memoria electrónica -20-, una interfaz -30- para introducir datos en el medio de almacenamiento (en el área de almacenamiento -20-) y para leer datos del medio de almacenamiento (del área de almacenamiento -20-), un dispositivo de introducción -70- acoplado entre la interfaz -30- y el área de almacenamiento -20- para almacenar datos de la interfaz -30- en el área de almacenamiento -20-, un dispositivo de lectura -80- acoplado entre la interfaz -30- y el área de almacenamiento -20- para emitir datos del área de almacenamiento -20- a la interfaz -30-, un dispositivo de autentificación -90- acoplado al dispositivo de lectura -80-, una memoria de clave -40- en la que está almacenada o se puede almacenar una clave secreta -K-, un dispositivo de cifrado -50- acoplado al dispositivo de introducción -70- para cifrar con la clave -K- datos introducidos a la interfaz -30- en el medio de almacenamiento -10- y un dispositivo de descifrado -60- acoplado al dispositivo de lectura -80- para descifrar con la clave -K- datos emitidos del área de almacenamiento -20-. El dispositivo de introducción -70- y el dispositivo de cifrado -50- no presentan una interfaz de usuario y por lo tanto no permiten al usuario elegir si los datos introducidos deben o no deben ser cifrados. El dispositivo de cifrado -50- realiza siempre el cifrado de datos que llegan de la interfaz -30-. El dispositivo de lectura -80- presenta un primer canal de lectura directo -A- y un segundo canal de lectura de descifrado -B-. En el segundo canal de lectura de descifrado -B- está integrado el dispositivo de autentificación -90-.

A la interfaz -30- del medio de almacenamiento -10- se puede acoplar un dispositivo de lectura/escritura (no mostrado) para medios de almacenamiento -10-, de forma que los datos puedan ser transferidos del dispositivo de lectura/escritura al medio de almacenamiento -10- y del medio de almacenamiento -10- al dispositivo de lectura/escritura.

La figura 2 muestra, en el medio de almacenamiento -10- de la figura 1, una introducción de datos -DAT- en un medio de almacenamiento -10-. Para mayor claridad, en las figuras 2-4 se han omitido algunos números de referencia. Los datos -DAT- son puestos a disposición del medio de almacenamiento -10- en la interfaz -30-. El dispositivo de introducción -70- suministra los datos -DAT- disponibles en la interfaz -30- al dispositivo de cifrado -50-, que cifra los datos -DAT- y los almacena como datos cifrados -FZXYZSS- en el área de almacenamiento -20-.

La figura 3 muestra una lectura de datos del medio de almacenamiento -10- de la figura 1 a través de un primer canal de lectura directo -A- del dispositivo de lectura -80-. A través de la interfaz -30- se introduce un comando de lectura -READ- en el medio de almacenamiento -10-. El dispositivo de lectura -80- procesa el comando de lectura -READ- y entrega los datos cifrados -FZXYZSS- a leer, por ejemplo, el contenido completo de la memoria del área de almacenamiento -20- o, dado el caso, el contenido de la memoria de un área de almacenamiento parcial seleccionable -20-, en forma cifrada, es decir, tal como está almacenado en el área de almacenamiento, a la interfaz -30-. Por lo tanto, en la interfaz -30- están disponibles datos cifrados -FZXYZSS- para ser recibidos por un dispositivo de lectura/escritura.

La figura 4 muestra una lectura de datos del medio de almacenamiento -10- de la figura 1 a través de un segundo canal de lectura de descifrado -B- del dispositivo de lectura -80-. A través de la interfaz 30- se introducen un comando de autentificación -AUT- y un comando de lectura -READ- en el medio de almacenamiento -10-. El dispositivo de lectura -80- procesa en primer lugar el comando de autentificación -AUT- y lo envía para su ejecución al dispositivo de autentificación -90-. El dispositivo de autentificación -90- ejecuta el comando de autentificación -AUT-. Si la autentificación realizada con el comando de autentificación -AUT- es exitosa, a continuación el dispositivo de lectura -80- procesa el comando de lectura -READ-. Los datos cifrados -FZXYZSS- a leer, por ejemplo, el contenido completo de la memoria del área de almacenamiento -20- o, dado el caso, el contenido de la memoria de un área de almacenamiento parcial seleccionable -20-, son transferidos al dispositivo de descifrado -60- y descifrados por el dispositivo de descifrado -60- para obtener datos descifrados - DAT-. Los datos -DAT- descifrados son puestos a disposición en la interfaz -30- para que puedan ser recibidos por un dispositivo de lectura/escritura.

En el modo de realización de la lectura de datos de la figura 4, el comando de autentificación -AUT- y el comando de lectura -READ- son introducidos mediante un único proceso de envío en la interfaz -30-. Para ello, por ejemplo, se solicita al usuario que se autentifique y su autentificación es valorada implícitamente como requisito para la lectura de datos. Alternativamente, en primer lugar se introduce el comando de autentificación -AUT- en la interfaz -30-, que es valorado por el dispositivo de lectura -80- y el dispositivo de autentificación -90-. En caso de una autentificación exitosa, el medio de almacenamiento -10- emite una confirmación de autentificación a la interfaz -30- y se solicita la introducción de un comando de lectura en la interfaz -30-. Cuando se introduce el comando de lectura -READ- en la interfaz -30-, los datos son descifrados tal como se ha descrito anteriormente y puestos a disposición de la interfaz -30- en forma descifrada -DAT- para ser recibidos por un dispositivo de lectura/escritura.

En caso de una autentificación fallida, opcionalmente se emiten datos cifrados, esencialmente como en el caso de una lectura sin autentificación, o alternativamente no se emite ningún dato.

REIVINDICACIONES

1. Medio de almacenamiento (10) con dispositivo de cifrado, con

- un área de memoria electrónica (20),
- una interfaz (30) para introducir datos en el medio de almacenamiento (10) y leer datos del medio de almacenamiento (10),
- un dispositivo de introducción (70) acoplado entre la interfaz (30) y el área de almacenamiento (20) para almacenar datos de la interfaz (30) en el área de almacenamiento (20),
- un dispositivo de lectura (80) acoplado entre la interfaz (30) y el área de almacenamiento (20) para emitir datos del área de almacenamiento (20) a la interfaz (30),
- una memoria de clave (40) en la que está almacenada o se puede almacenar una clave secreta (K),
- un dispositivo de cifrado (50) acoplado al dispositivo de introducción (70) para cifrar con la clave (K) datos introducidos a la interfaz (30) en el medio de almacenamiento (10), y
- un dispositivo de descifrado (60) acoplado al dispositivo de lectura (80) para descifrar datos emitidos desde el área de almacenamiento (20),
- el dispositivo de lectura (80) comprendiendo:

    - un canal de lectura de descifrado (B) configurado para poder descifrar datos almacenados cifrados en el área de almacenamiento (20) utilizando el dispositivo de descifrado (60) con la clave (K) almacenada en la memoria de clave (40), o una clave de descifrado correspondiente a la clave (K) y almacenada en la memoria de clave (40), y poder emitirlos de forma descifrada a la interfaz (30) mediante el canal de lectura de descifrado (B) y

- el medio de almacenamiento comprendiendo además un dispositivo de autentificación acoplado al dispositivo de lectura (80), estando configurado el dispositivo de autentificación tal que

los datos pueden ser emitidos de forma descifrada a la interfaz (30) mediante el canal de lectura de descifrado (B) como mucho en caso de una autentificación exitosa,

caracterizado por que

- el dispositivo de introducción (70) está configurado para cifrar todos los datos introducidos a la interfaz (30) para su almacenamiento en el área de almacenamiento (20) con la clave (K) almacenada en la memoria de clave (40) y almacenarlos cifrados en el área de almacenamiento (20), y

- el dispositivo de lectura (80) comprende además:

    - un canal de lectura directo (A) configurado para emitir los datos almacenados cifrados en el área de almacenamiento (20) de forma cifrada a la interfaz (30), evitando el dispositivo de descifrado (60), mediante el canal de lectura directo (A), y

- los datos se pueden emitir de forma cifrada mediante el canal de lectura directo (A) en caso de no producirse o fallar una autentificación.

2. Medio de almacenamiento (10), según la reivindicación 1, en el que el área de almacenamiento (20) está configurada al menos parcialmente como memoria Flash.

3. Medio de almacenamiento (10), según cualquiera de las reivindicaciones 1 a 2, en el que como clave (K) está prevista una clave simétrica de un sistema de cifrado simétrico.

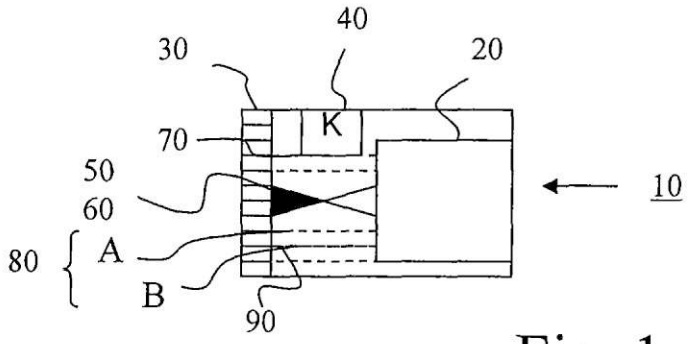

Fig. 1

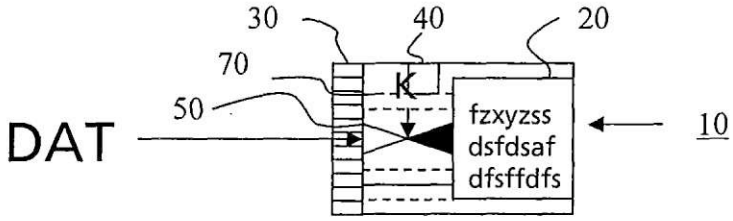

Fig. 2

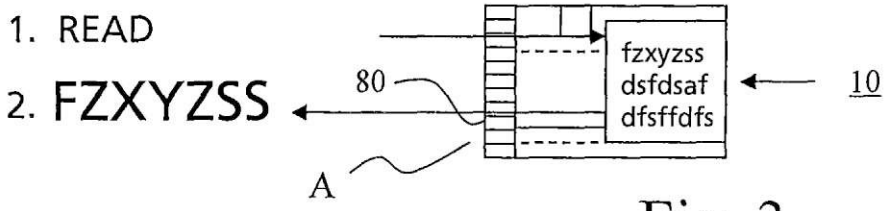

Fig. 3

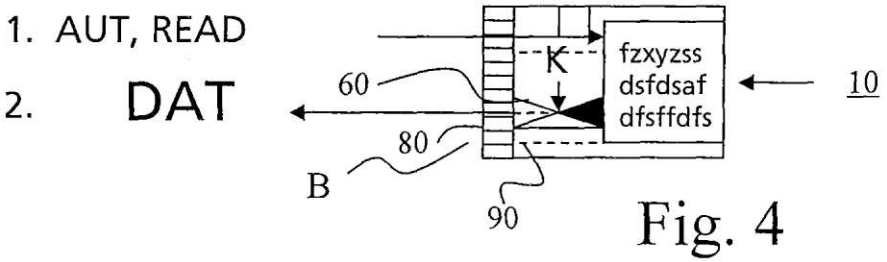

Fig. 4

Fig. 5