(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 721 250**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.11.2016 E 16197434 (0)**

(97) Fecha y número de publicación de la concesión europea: **23.01.2019 EP 3166252**

(54) Título: **Procedimiento de grabación segura de datos, dispositivo y programa correspondientes**

(30) Prioridad:

06.11.2015 FR 1560682

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.07.2019

(73) Titular/es:

INGENICO GROUP (100.0%)
28/32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

ROYER, JESSICA;
BELLAHCENE, MOHAMMED;
POMMARET, JEAN-CHRISTOPHE;
ROLIN, CHRISTIAN y
MULLER, LAURENT

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de grabación segura de datos, dispositivo y programa correspondientes

1. Campo

La invención se refiere al campo del refuerzo de la seguridad de datos y, más en particular, trata de la grabación segura de datos en un dispositivo de grabación de datos.

2. Técnica anterior

La grabación de datos en los terminales y equipos informáticos tales como ordenadores, servidores, teléfonos móviles, objetos conectados, etc. presenta, a día de hoy, un reto capital, dada la actual omnipresencia de este tipo de aparatos y el continuo crecimiento del volumen de datos generados diariamente tanto en el ámbito profesional como doméstico. Para responder a esta problemática de grabación de datos, se han realizado notorios progresos en la capacidad de las memorias para grabar un gran volumen de datos en un reducido espacio.

Existe, a día de hoy, una necesidad más en particular para grabar en memoria de manera segura datos sensibles cuyo acceso se desea controlar. Así, se han desarrollado en los últimos años técnicas de cifrado para garantizar la confidencialidad de los datos grabados en los dispositivos de grabación de datos. De este modo, a día de hoy, se ponen en práctica asiduamente mecanismos de identificación y/o de autenticación para controlar el acceso a datos sensibles en la memoria de un terminal. Así, estas memorias, llamadas memorias seguras o memorias protegidas, permiten a un usuario grabar datos en vistas a acceder a ellos posteriormente con total seguridad.

La puesta en práctica de tales memorias seguras en terminales, tales como, por ejemplo, un ordenador o un teléfono móvil, presenta, no obstante, ciertos problemas. Los datos sensibles son grabados generalmente en memorias seguras de pequeño tamaño, presentando la puesta en práctica de estas memorias un importante coste con respecto a una memoria convencional no protegida. Según es sabido, un terminal puede comprender un área de memoria segura en la que se graban los datos más sensibles de un usuario, así como un área de memoria no segura en la que se graba el resto de los datos que no presentan un particular riesgo de seguridad. Este tipo de organización lo hallamos, por ejemplo, convencionalmente, en los terminales de pago que comprenden una memoria protegida para grabar datos confidenciales y una memoria no protegida para grabar datos menos sensibles.

El reducido tamaño de las áreas de memoria seguras en los terminales y, de manera más general, en los dispositivos de grabación de datos, plantea un problema a día de hoy, por cuanto que no siempre se dispone del espacio de memoria segura necesario para grabar el conjunto de los datos sensibles cuyo acceso se desea proteger.

El uso creciente de datos confidenciales en los equipos y procesos modernos reclama consiguientemente una nueva solución que garantice una grabación segura para un gran volumen de datos en un dispositivo de grabación de datos, al propio tiempo que limite el uso de espacio de memoria seguro. Existe, además, una necesidad de una solución de grabación segura que asegure de manera fiable la integridad de los datos sensibles, especialmente en el acceso por parte de un usuario a los datos en cuestión.

Y. Hu, G. Hammouri, B. Sunar: "A Fast Real-time Memory Authentication Protocol", Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing, STC'08, expone el uso de un árbol de obtención de resumen parcialmente almacenado en una memoria protegida con el fin de reforzar la seguridad de la integridad de un conjunto de datos.

El documento de publicación de solicitud de patente US 2002/147918 A1, Osthoff et al., expone el almacenamiento de un identificador de dispositivo, de un valor calculado aplicando una función resumen sobre dicho identificador y de dicha propia función resumen en una memoria segura.

3. Resumen

Es una de las finalidades de la invención subsanar las insuficiencias e inconvenientes del estado de la técnica.

A tal efecto, la divulgación propone un procedimiento de grabación segura de datos, puesto en práctica en un dispositivo de grabación de datos que comprende una primera memoria no segura y una segunda memoria segura, comprendiendo el procedimiento las siguientes etapas:

- obtención, a partir de una clave madre grabada en la segunda memoria, de una clave derivada correspondiente a los datos grabados en la segunda memoria;

- cifrado, a partir de la clave derivada, de los datos suministrando datos cifrados;

- grabación de los datos cifrados en la primera memoria;

- determinación de una huella de resumen de dichos datos;

- grabación de dicha huella de resumen, en asociación con los datos, en un fichero de resumen grabado en la primera memoria;

- grabación, en la segunda memoria, de una huella de resumen general representativa del contenido del fichero de resumen que comprende dicha huella de resumen; y

- supresión de los datos de la segunda memoria con posterioridad a dicha grabación de los datos cifrados en la primera memoria.

La presente técnica permite ventajosamente grabar datos de manera segura en el dispositivo de grabación de datos, al propio tiempo que limita el espacio de memoria utilizado al efecto en la memoria segura de dicho dispositivo. Para conseguir esto, los datos se graban de forma cifrada en la memoria no segura. Estos mismos datos se retiran de la memoria segura M2 con el fin de ganar espacio de memoria. La clave madre, a partir de la cual son cifrados los datos, se graba en la memoria segura del dispositivo de grabación de datos a fin de proteger el acceso a dicha clave madre.

Como se explica en lo sucesivo, la puesta en práctica y la grabación del fichero de resumen y de la huella de resumen general permiten además controlar de manera fiable la integridad de los datos grabados de forma cifrada en la memoria no segura.

De acuerdo con una forma particular de realización, después de su obtención, la clave derivada es grabada en la segunda memoria, comprendiendo además el procedimiento una etapa de supresión de la clave derivada de la segunda memoria tras el cifrado de dichos datos. Así, todavía es posible ahorrar más espacio en la memoria segura del dispositivo de grabación de datos.

De acuerdo con una forma particular de realización, la clave madre es generada de manera aleatoria de una vez por todas en el dispositivo de grabación de datos. De esta manera, le es más difícil a un tercero malintencionado recuperar la clave madre de manera fraudulenta.

De acuerdo con una forma particular de realización, en la etapa de obtención, la clave derivada se obtiene a partir:

- de un identificador de usuario representativo de un usuario del dispositivo de grabación de datos; y

- de un identificador de los datos.

Así, de acuerdo con una característica particular, la clave derivada está vinculada a un usuario y a los datos en cuestión.

De acuerdo con una forma particular de realización, en dicha grabación de los datos cifrados, dichos datos cifrados se graban en la primera memoria en forma de un fichero cifrado al que se atribuye un nombre de fichero que comprende el identificador de usuario y el identificador de los datos. Así, es posible hallar con facilidad un fichero cifrado que comprende, de forma cifrada, datos a los que se pretende acceder.

De acuerdo con una forma particular de realización, el procedimiento comprende, a continuación de dicha grabación de la huella de resumen en el fichero de resumen, una grabación de una copia del fichero de resumen en una memoria segura de copia de seguridad del dispositivo de grabación de datos. En un ejemplo particular, esta memoria de copia de seguridad está comprendida en la segunda memoria segura. Si posteriormente se detecta que el fichero de resumen grabado en la primera memoria no está íntegro, el dispositivo de grabación puede recuperar entonces de manera segura la copia del fichero de resumen de la memoria de copia de seguridad. En un ejemplo particular, en caso de detección de una vulneración de la integridad del fichero de resumen en la primera memoria, el dispositivo de grabación sustituye entonces dicho fichero de resumen en la primera memoria por dicha copia proveniente de la memoria de copia de seguridad.

La divulgación propone asimismo un procedimiento de recuperación segura de datos, puesto en práctica en un dispositivo de grabación de datos que comprende una primera memoria no segura y una segunda memoria segura, comprendiendo el procedimiento:

- una verificación de la integridad de un fichero de resumen grabado en la primera memoria, a partir de una huella de resumen general grabada en la segunda memoria;

- y luego, si el fichero de resumen se detecta como íntegro, el procedimiento comprende además, a la recepción de una petición de acceso a datos, las siguientes etapas:

  - obtención, a partir de una clave madre grabada en la segunda memoria, de una clave derivada correspondiente a datos cifrados grabados en la primera memoria;

  - descifrado, a partir de la clave derivada obtenida, de los datos cifrados a fin de recuperar dichos datos;

  - grabación de dichos datos en la segunda memoria;

- determinación de la huella de resumen de dichos datos;

- verificación de la integridad de los datos grabados en la segunda memoria comparando la huella de resumen determinada para los datos con una huella de resumen grabada en el fichero de resumen en asociación con dichos datos; y

- autorización de un acceso a los datos en la segunda memoria como respuesta a dicha petición de acceso, solamente si los datos se han determinado como íntegros.

Así, la presente técnica permite acceder a los datos grabados en la memoria no segura sin comprometer la confidencialidad de dichos datos. En el procedimiento de recuperación segura de datos, en ningún momento los datos se hallan presentes de forma no cifrada (en claro) en la memoria no segura. La invención permite además verificar de manera fiable la integridad de los datos a los que se accede a conveniencia en la memoria segura.

De acuerdo con una forma particular de realización, el procedimiento comprende una etapa de obtención de un identificador de usuario representativo de un usuario del dispositivo de grabación de datos y de un identificador de los datos, en el que la clave derivada se obtiene a partir de la clave madre utilizando el identificador de usuario y el identificador de los datos.

De manera ventajosa, por cuanto que el identificador de usuario y el identificador de datos son constantes, la clave derivada determinada a partir de la clave madre es siempre la misma.

De acuerdo con una forma particular de realización, el procedimiento comprende, con posterioridad a un acceso a los datos, la ejecución unas de etapas de cifrado de los datos a datos cifrados, de grabación de los datos cifrados, de determinación de una huella de resumen, de grabación de la huella de resumen, de grabación de la huella de resumen general y de supresión de los datos, tales y como se han definido anteriormente en el procedimiento de grabación segura.

La invención permite entonces ventajosamente grabar de manera segura, en la memoria no segura, datos a los que se ha accedido en la memoria segura.

De acuerdo con una forma particular de realización, el procedimiento comprende además, con posterioridad a un acceso del usuario a los datos en la segunda memoria, las siguientes etapas:

- determinación de una segunda huella de resumen de dichos datos a continuación de dicho acceso; y

- comparación de dicha segunda huella de resumen con la huella de resumen grabada en el fichero de resumen en asociación con los datos, con el fin de detectar si los datos han sido modificados en dicho acceso;

en el que el procedimiento comprende la ejecución de unas etapas de cifrado, de grabación de los datos cifrados, de determinación de una huella de resumen, de grabación de dicha huella de resumen y de grabación de un valor de resumen general, tales y como se han definido anteriormente en el procedimiento de grabación segura, únicamente si se detecta que los datos han sido modificados en dicho acceso.

Así, se puede evitar la repetición superflua de ciertas etapas del procedimiento de grabación segura a continuación de un acceso a datos en la memoria segura del terminal. De ello resulta una ganancia de tiempo y de eficiencia, así como un ahorro de los recursos utilizados en el dispositivo de grabación de datos.

En una forma particular de realización, las diferentes etapas del procedimiento de grabación segura de datos y del procedimiento de recuperación segura de datos vienen determinadas por instrucciones de programas de ordenador.

De este modo, la presente técnica también tiene como propósito un programa de ordenador en un soporte de información (o soporte de grabación), siendo susceptible este programa de ser puesto en práctica en un dispositivo de grabación de datos o, de manera más general, en un ordenador, incluyendo este programa unas instrucciones adaptadas para la puesta en práctica de las etapas de un procedimiento de grabación segura de datos y/o de un procedimiento de recuperación segura de datos, tales y como se han definido anteriormente.

Este programa puede utilizar cualquier lenguaje de programación y presentarse en forma de código fuente, código objeto, o de código intermedio entre código fuente y código objeto, tal como en una forma compilada parcialmente, o en cualquier otra forma deseable.

La invención también tiene como propósito un soporte de información (o soporte de grabación) legible por ordenador, y que incluye instrucciones de un programa de ordenador tal y como se ha mencionado anteriormente.

El soporte de información puede ser cualquier entidad o dispositivo capaz de grabar el programa. Por ejemplo, el soporte puede comprender un medio de grabación, tal como una ROM, por ejemplo un CD-ROM o una ROM de circuito microelectrónico, o también un medio de grabación magnética, por ejemplo un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de información puede ser un soporte transmisible, tal como una señal eléctrica u óptica, que se puede conducir a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención se puede descargar en particular en una red de tipo Internet.

Alternativamente, el soporte de información puede ser un circuito integrado en el que va incorporado el programa, estando adaptado el circuito para ejecutar o para ser utilizado en la ejecución de al menos uno cualquiera de los procedimientos en cuestión.

La presente técnica trata además de un dispositivo de grabación de datos que comprende:

- una primera memoria no segura;

- una segunda memoria segura;

- un módulo de obtención para obtener, a partir de una clave madre grabada en la segunda memoria, una clave derivada correspondiente a datos grabados en la segunda memoria;

- un módulo de cifrado para cifrar, a partir de la clave derivada, dichos datos al objeto de suministrar datos cifrados;

- un primer módulo de grabación para grabar los datos cifrados en la primera memoria;

- un módulo de determinación para determinar una huella de resumen de dichos datos;

- un segundo módulo de grabación para grabar dicha huella de resumen, en asociación con los datos, en un fichero de resumen grabado en la primera memoria;

- un tercer módulo de grabación para grabar, en la segunda memoria, una huella de resumen general representativa del contenido del fichero de resumen que comprende dicha huella de resumen; y

- un módulo de supresión para suprimir los datos de la segunda memoria con posterioridad a dicha grabación de los datos cifrados en la primera memoria.

De acuerdo con una forma particular de realización, dicho dispositivo es tal que:

- el módulo de obtención está configurado para grabar, en la segunda memoria, la clave derivada obtenida a partir de la clave madre; y

- el módulo de supresión está configurado para suprimir la clave derivada grabada en la segunda memoria después del cifrado de dichos datos por el módulo de cifrado.

Nótese que las diferentes formas de realización definidas anteriormente en relación con el procedimiento de grabación segura de datos y con el procedimiento de recuperación segura de datos, como igualmente las ventajas asociadas a estos procedimientos, se aplican por analogía al dispositivo de grabación segura de la invención.

De acuerdo con una forma de realización, la invención se lleva a la práctica por medio de componentes de soporte lógico y/o de soporte físico. En esta línea, el término "módulo" puede corresponder, en este documento, tanto a un componente de soporte lógico, como a un componente de soporte físico o a un conjunto de componentes de soporte físico y lógico.

Un componente de soporte lógico corresponde a uno o varios programas de ordenador, uno o varios subprogramas de un programa o, de manera más general, a todo elemento de un programa o de un soporte lógico apto para llevar a la práctica una función o un conjunto de funciones, según lo descrito a continuación en relación con el módulo de que se trate. Tal componente de soporte lógico es ejecutado por un procesador de datos de una entidad física (terminal, servidor, pasarela, encaminador, etc.) y está posibilitado de acceso a los recursos de soporte físico de esta entidad física (memorias, soportes de grabación, buses de comunicación, tarjetas electrónicas de entrada/salida, interfaces de usuario, etc.).

De la misma manera, un componente de soporte físico corresponde a todo elemento de un conjunto de soporte físico (o hardware) apto para llevar a la práctica una función o un conjunto de funciones, según lo descrito a continuación en relación con el módulo de que se trate. Puede ser un componente de soporte físico programable o con procesador integrado para la ejecución de soporte lógico, por ejemplo un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microprograma (firmware), etc.

Por supuesto, cada componente del sistema anteriormente descrito pone en práctica sus propios módulos de lógica.

Nótese, por otro lado, que las diferentes formas de realización antes mencionadas son combinables entre sí para la puesta en práctica de la invención.

4. Figuras

Otras características y ventajas de la presente técnica se desprenderán de la descripción que se realiza a continuación, con referencia a los dibujos que se acompañan, los cuales, sin carácter limitativo alguno, ilustran ejemplos de realización de la misma. En las figuras:

- la figura 1 presenta esquemáticamente la estructura de un dispositivo de grabación segura de datos, según una forma particular de realización;

- la figura 2 representa esquemáticamente módulos puestos en práctica en el dispositivo de grabación de datos representado en la figura 1;

- la figura 3 representa, en forma de un organigrama, las etapas de un procedimiento de grabación segura de datos, según una forma particular de realización de la invención;

- la figura 4 representa, en forma de un organigrama, las etapas de un procedimiento de recuperación segura de datos, según una forma particular de realización de la invención;

- la figura 5 representa, en forma de un organigrama, un procedimiento de grabación segura de datos, según una forma particular de realización de la invención; y

- la figura 6 representa, en forma de un organigrama, un procedimiento de grabación segura de datos, según otra forma de realización de la invención.

5. Descripción

Como se ha indicado anteriormente, la invención concierne al refuerzo de la seguridad de datos y, más en particular, trata de la grabación segura de datos en un dispositivo de grabación de datos.

Como se ha expuesto previamente, el principio general de la técnica que se propone radica en la utilización de un dispositivo de grabación de datos que comprende una primera memoria no segura y una segunda memoria segura, con el fin de grabar datos de manera segura. Más en particular, consiste el principio en grabar datos de forma cifrada en la memoria no segura, de modo que estos datos sean accesibles a conveniencia sin comprometer su confidencialidad. Cuando no se necesita ningún acceso a estos datos, estos datos no están presentes en la memoria segura del dispositivo, con el fin de ahorrar espacio de memoria en esta memoria segura. Si, en cambio, se necesita el acceso a los datos, los datos cifrados grabados en la memoria no segura se descifran y graban provisionalmente en la memoria segura con el fin de permitir el acceso a los datos, al propio tiempo que se garantiza la confidencialidad de los mismos. En el dispositivo de grabación se puede poner en práctica además un mecanismo de verificación de la integridad con el fin de verificar que los datos que se descifran en la memoria segura están íntegros.

Los datos cuyo acceso se hace seguro con ayuda de la invención pueden ser cualesquiera, especialmente en cuanto a naturaleza y a forma.

Otros aspectos y ventajas de la presente técnica se irán desprendiendo de los ejemplos de realización que a continuación se describen con referencia a los dibujos mencionados anteriormente.

Salvo que se indique lo contrario, los elementos comunes o análogos en varias figuras llevan los mismos signos de referencia y presentan características idénticas o análogas, de modo que estos elementos comunes generalmente no se describen nuevamente en interés de la simplicidad.

La figura 1 representa, de manera esquemática, la estructura de un dispositivo de grabación de datos 2 conforme a una forma particular de realización. El dispositivo 2 (denominado en lo sucesivo “terminal”) es, en este caso particular, un terminal de pago, pudiéndose contemplar, por supuesto, otros ejemplos dentro del ámbito de la invención.

Se hace notar que ciertos constituyentes que generalmente forman parte de un terminal, tal como un terminal de pago, se han omitido voluntariamente, pues no son necesarios para la comprensión de la presente técnica.

Más en particular, el terminal 2 comprende, en este punto, una unidad de control 4 y memorias no volátiles 5, 6, M1 y M2.

La memoria 5 es una memoria no volátil regrabable o una memoria de sólo lectura (ROM), constituyendo esta memoria un soporte de grabación conforme a una forma particular de realización de la invención, legible por el terminal 2, y en el que está grabado un programa de ordenador PG conforme a una forma particular de realización de la invención. Este programa de ordenador PG comprende instrucciones para la ejecución de las etapas de un procedimiento de grabación segura de datos y de un procedimiento de recuperación segura de datos, según una forma particular de realización de la invención. Las principales etapas de estos procedimientos se representan en la figura 3 que posteriormente se describe.

La unidad de control 4 (un procesador en este ejemplo), pilotada por el programa de ordenador PG, pone en práctica en este punto cierto número de módulos representados en la figura 2, a saber: un módulo de obtención MO, un módulo de cifrado ME, un módulo de determinación MD, un primer módulo de grabación MST1, un segundo módulo de grabación MST2, un tercer módulo de grabación MST3 y un módulo de supresión MS. Posteriormente se describirá un ejemplo de puesta en práctica de estos módulos.

Adicionalmente, el procesador 4 es apto para recibir como entrada un identificador de usuario UID y un identificador DID de datos. El uso de los identificadores UID y DID se describirá posteriormente en detalle en una puesta en práctica particular.

La memoria M2 es una memoria segura (o protegida). Se entiende, en la presente exposición, por “memoria segura”, una memoria cuyo contenido tiene el acceso protegido por un mecanismo de seguridad conveniente. Tal mecanismo permite, por ejemplo, verificar la identidad y/o la autenticidad de un peticionario que pretenda acceder a datos grabados en la memoria segura en cuestión. Típicamente, una memoria segura está ligada a un procesador seguro apto para llevar a la práctica un mecanismo de refuerzo de la seguridad de los datos en la memoria, que comprende, por ejemplo, el borrado de los datos en caso de vulneración de la integridad de los datos. El mecanismo de seguridad puede asimismo ser soporte físico (capa física que recubre la memoria para proteger la lectura de la misma...).

La memoria 6 es una memoria no volátil regrabable que sirve de memoria de copia de seguridad (o “back-up”). Se comprenderá, no obstante, que la utilización de tal memoria de copia de seguridad no es obligatoria para poner en práctica la invención.

En el ejemplo de que se trata en este punto, la memoria de copia de seguridad 6 es una memoria segura de la misma manera que la memoria M2. La memoria 6 puede estar comprendida en la memoria segura M2 o, alternativamente, ser externa a la memoria segura M2.

La memoria M1, en cambio, es una memoria no segura. En otras palabras, el acceso al contenido de la memoria M1 no está protegido, a diferencia del acceso al contenido de la memoria M2.

La memoria M1 es apta para grabar datos DD de forma cifrada (señalados con CD en la forma cifrada), por ejemplo en forma de al menos un fichero cifrado CF, con el fin de impedir el acceso a dichos datos DD a toda persona no autorizada. No obstante, se comprenderá que dichos datos cifrados CD en la memoria M1 no tienen que ser grabados obligatoriamente en forma de fichero. Cabe contemplar, en efecto, dentro del ámbito de la presente técnica, grabar, en la memoria no segura M1, datos cifrados CD que no se materialicen en forma de un fichero. Se supondrá, no obstante, en los ejemplos de realización que siguen, que cada dato cifrado CD grabado en la memoria no segura M1 está contenido en un fichero cifrado CF.

Se asume, por ejemplo, el caso en que la memoria M1 comprende un fichero cifrado CF1 que contiene datos cifrados CD1, así como un fichero cifrado CF2 que contiene datos cifrados CD2. En este ejemplo, los datos cifrados CD1 y CD2 son, respectivamente, los datos DD1 y DD2 de forma cifrada.

Por otro lado, se atribuye un nombre de fichero N1, N2 respectivamente al fichero cifrado CF1, CF2. Siempre en este ejemplo, cada nombre de fichero comprende el identificador de usuario UID de un usuario y el identificador DID de los datos DD contenidos de forma cifrada en el fichero CF en cuestión. En este ejemplo, el nombre de fichero N1 comprende el identificador de usuario UID y el identificador DID2 de datos DD1. Igualmente, el nombre de fichero N2 comprende, en este punto, el mismo identificador de usuario UID y el identificador DID2 de datos DD2.

La memoria M1 comprende además un fichero de resumen HF en el que se puede grabar una respectiva huella de resumen H en asociación con cada dato DD (o conjunto de datos) de la memoria M2 grabado de forma cifrada en la memoria M1. Cada huella de resumen (o “valor de hash”) se obtiene aplicando una función resumen a los correspondientes datos DD. La misma función resumen es utilizada para determinar la huella de resumen de cada conjunto de datos que se graba de forma cifrada en la memoria no segura M1. Así, una huella de resumen H es representativa de los datos contenidos en el fichero cifrado CF de que se trate, sin que sea posible determinar, a partir de esta huella de resumen, ni el contenido del fichero CF en cuestión, ni su valor en claro. En el ejemplo representado en la figura 1, el fichero de resumen HF comprende la huella de resumen H1 asociada a los datos DD1, así como la huella de resumen H2 asociada a unos datos DD2.

La memoria segura M2 es apta, por otro lado, para grabar datos DD cuya confidencialidad se pretende preservar. Los datos DD son grabados, en este punto, en la memoria segura M2 de forma no cifrada en ficheros no cifrados DF. Como se indica en lo sucesivo, se considera, por ejemplo, un estado inicial en el que el fichero no cifrado DF1 que incluye unos datos DD1 es grabado en la memoria M2.

Se comprenderá, no obstante, que dichos datos DD no tienen que ser grabados obligatoriamente en forma de fichero en la grabación en la memoria segura M2. Cabe contemplar, en efecto, dentro del ámbito de la presente técnica, grabar en la memoria segura M2 unos datos DD que no se materialicen en forma de un fichero. Se supondrá, no obstante, en los ejemplos de realización que siguen, que cada dato DD grabado en la memoria M2 está contenido en un fichero DF.

La memoria M2, por otro lado, es apta para grabar una clave criptográfica madre RK, una clave criptográfica (señalado, por ejemplo, con DK1) derivada de la clave madre RK, así como una huella de resumen general GHV. El objeto y el uso de estos parámetros se describirán con mayor detalle posteriormente en una puesta en práctica particular.

Más en particular, la huella de resumen general GHV es una huella de resumen obtenida aplicando una función resumen a partir del contenido del fichero de resumen HF. De este modo, el valor de GHV en un momento dado es representativo del contenido del fichero de resumen HF en el momento de que se trate. Por lo tanto, toda adición, supresión o modificación de una huella de resumen H en el fichero de resumen HF tiene como consecuencia el modificar el valor de GHV en la memoria M2, como se explica con mayor detalle en lo sucesivo.

Con referencia a la figura 3, ahora se describe una forma particular de realización de la invención. Más concretamente, el terminal 2 pone en práctica un procedimiento de grabación segura de datos ejecutando el programa de ordenador PG.

Se considera un estado inicial en el que un fichero no cifrado DF1 que incluye unos datos DD1 en estado no cifrado es grabado en la memoria segura M2. Se supone, adicionalmente, que en la memoria M1 no se graba ningún fichero cifrado CF y que el fichero de resumen HF está vacío.

Se supone, por otro lado, que la clave criptográfica madre RK es generada previamente en el terminal 2, por ejemplo de manera aleatoria, y grabada en la memoria M2 como se ha indicado anteriormente. En un ejemplo particular, la clave madre RK es generada aleatoriamente de una vez por todas en la vida útil del terminal 2.

En una etapa de obtención S2, el procesador 4 obtiene un identificador de usuario UID de un usuario del terminal 2, así como un identificador DID1 de los datos DD1. En un ejemplo particular, el terminal 2 puede recibir los identificadores UID y DID1 desde el exterior de dicho terminal. Alternativamente, el terminal 2 puede determinar al menos uno de entre los identificadores UID y DID1. La determinación por parte del terminal 2 especialmente del identificador de usuario UID1 permite impedir que un tercero acceda a los datos DD de otro usuario en el terminal T1. La manera en que el procesador 4 determina o recupera el identificador de usuario UID1 y el identificador DID1 se podrá adaptar según el contexto de utilización.

El módulo de obtención MO determina (S4) a continuación, a partir de la clave madre RK grabada en la memoria segura M2, una clave criptográfica DK1, llamada “clave derivada”, correspondiente a los datos DD1 grabados en la memoria M2. En el ejemplo contemplado en este punto, el módulo de obtención MO obtiene la clave derivada DK1 a partir de la clave madre RK utilizando el identificador de usuario UID y el identificador DID1 de los datos DD1.

El módulo de obtención MO graba (S6) además la clave derivada DK1 en la memoria segura M2, con el fin de que esta clave DK1 pueda utilizarse posteriormente.

En el curso de una etapa de cifrado S8, el módulo de cifrado ME cifra (S8), a partir de la clave derivada DK1, el fichero DF1 que incluye los datos DD1 a fin de obtener un fichero cifrado CF1 que incluye los datos DD1 de forma cifrada (señalados con CD1). Para conseguir esto, el módulo de cifrado ME utiliza, por ejemplo, un algoritmo de cifrado simétrico para cifrar el fichero DF1. No obstante, cabría contemplar la posibilidad de un algoritmo de cifrado asimétrico dentro del ámbito de la invención. Se supondrá en este punto que se utiliza el mismo algoritmo de cifrado para cifrar cada fichero de datos en este procedimiento.

El fichero cifrado CF1 es grabado (S10) por el primer módulo de grabación MST1 en la memoria M1. En el ejemplo descrito en este punto, se atribuye al fichero cifrado CF1 el nombre N1 que comprende el identificador de usuario UID y el identificador DID1 de los datos DD1.

El módulo de determinación MD determina (S12), por otro lado, una huella de resumen H1 de los datos DD1 comprendidos de forma no cifrada en el fichero DF1. Como ya se ha explicado, esta huella de resumen H1 es representativa de los datos DD1 contenidos en el fichero no cifrado DF1.

La huella de resumen H1 es grabada (S14) además por el segundo módulo de grabación MST2, en el fichero de resumen HF, en asociación con los datos DD1. En un caso particular, cada huella de resumen H grabada en el fichero de resumen HF está asociada al identificador DID de los datos DD correspondientes (es decir, DID1 en el presente caso).

De acuerdo con una variante de realización, a continuación de la etapa de grabación S14, el procesador 4 puede además grabar una copia del fichero de resumen HF en la memoria segura de copia de seguridad 6. Esta copia de seguridad permite, de ser necesario, recuperar posteriormente de manera segura la huella de resumen H1, como se describe en lo sucesivo.

Siempre en la forma de realización que en este punto se contempla, una vez realizada la etapa S14, el tercer módulo de grabación MST3 determina y luego graba (S16), en la memoria segura M2, una huella de resumen general GHV representativa del contenido del fichero de resumen HF en el que ahora se encuentra la huella de resumen H1. En el supuesto de que la huella de resumen general GHV ya tiene cualquier valor previamente a la

etapa S16, este valor es actualizado por el tercer módulo de grabación MST3 en la etapa S16.

En el curso de una etapa de supresión S18, el módulo de supresión MS suprime el fichero no cifrado DF1 de la memoria segura M2 al objeto de dejar en ella espacio de memoria. En un ejemplo particular, el módulo de supresión MS suprime (S18) además, después de la etapa de cifrado S8, la clave derivada DK1 de la memoria segura M2, al objeto de dejar en ella todavía más espacio de memoria.

Se comprenderá que la puesta en práctica de esta forma de realización no se limita al orden de ejecución tal y como se representa en la figura 3. En particular, las etapas S12 a S16 se pueden realizar antes de las (o paralelamente a las) etapas S6-S10, e incluso antes de (paralelamente a) la etapa S4.

Así, la presente técnica permite grabar datos de manera segura en el terminal 2, al propio tiempo que limita el espacio de memoria utilizado al efecto en la memoria segura M2. Para conseguir esto, los datos se graban de forma cifrada en la memoria no segura. Estos mismos datos se retiran de la memoria segura M2 con el fin de ganar espacio de memoria. La clave madre, a partir de la cual se cifran los datos, se graba en la memoria segura del terminal, de modo que a un tercero malintencionado no le es posible descifrar fácilmente los datos grabados de forma cifrada en la memoria no segura M1.

Como se explica en lo sucesivo, la puesta en práctica y la grabación del fichero de resumen HF y de la huella de resumen general GHV (respectivamente en M1 y M2) permiten además controlar de manera fiable la integridad de los datos grabados de forma cifrada en la memoria no segura M1.

A continuación del procedimiento de grabación segura S4-S18 antes descrito, un usuario puede ventajosamente acceder a unos datos DD presentes de forma cifrada en la memoria no segura M1 sin hacer peligrar la confidencialidad de dichos datos.

Para este fin, se describe ahora, con referencia a la figura 4, un procedimiento de recuperación segura de datos S38-S48 posterior al procedimiento de grabación segura S4-S18, siendo puesto en práctica este procedimiento de recuperación segura de datos por el terminal 2 según una forma particular de realización. En el ejemplo descrito en este punto, el terminal 2 pone en práctica un procedimiento de recuperación segura de datos ejecutando el programa de ordenador PG.

Más específicamente, con posterioridad al procedimiento de grabación segura S4-S18, el procesador 4 verifica (S30) la integridad del fichero de resumen HF a partir de la huella de resumen general GHV grabada en la memoria segura M2. Para conseguir esto, el procesador 4 calcula la huella de resumen general del fichero de resumen HF y verifica que la huella de resumen general así calculada concuerda con la huella de resumen general GHV grabada en la memoria segura M2. En un ejemplo particular, el procesador 4 procede sistemáticamente a la etapa S30 en el inicio del terminal 2 o de una aplicación particular puesta en práctica en el terminal 2.

En caso de concordancia en la etapa de verificación S30, el procesador 4 pone en práctica la etapa de determinación del acceso a los datos S32. En caso contrario, el procesador 4 pone en práctica la etapa de determinación de que el fichero de resumen HF es inválido. Tal ausencia de concordancia refleja una probable alteración (eventualmente malintencionada) del fichero de resumen HF entre la etapa de grabación S14 del fichero de resumen HF tal y como se ha descrito anteriormente y la presente verificación S30.

Como se ha indicado anteriormente, de acuerdo con una variante de realización, el procesador 4 puede haber grabado previamente una copia del fichero de resumen HF en la memoria segura de copia de seguridad 6, a continuación de la etapa de grabación S14. En este caso, a continuación de la etapa S34 de detección de la invalidez del fichero de resumen HF en la memoria M1, el procesador 4 puede recuperar (S36) entonces, en la memoria de copia de seguridad 6, dicha copia del fichero de resumen HF. Una vez efectuada esta recuperación S36, el procesador 4 puede estar configurado para sustituir el fichero de resumen HF inválido contenido en la memoria no segura M1 por la copia del fichero de resumen HF proveniente de la memoria de copia de seguridad 6. El procesador 4 puede proceder a continuación a las etapas S32 y siguientes según se describen seguidamente. Así, al ser segura, en este punto, la memoria de copia de seguridad 6, el procesador 4 tiene la capacidad de recuperar una copia íntegra del fichero de resumen HF en caso de vulneración de la integridad del fichero de resumen original grabado en la memoria no segura M1.

En la etapa de determinación S32, el procesador 4 determina si se requiere el acceso a los datos cifrados CD1 grabados en la memoria M1. Cuando es recibida por el procesador 4 una petición de acceso RQ a los datos DD1, este último procede a las etapas S38-S52 que pasamos a describir con referencia a la figura 4.

Se supone en este punto que la petición de acceso RQ recibida por el terminal 2 comprende el identificador de usuario UID y el identificador DID1 de los datos DD1 a los que pretende acceder un usuario autorizado (aquél identificado por UID).

En el curso de una etapa de recuperación S38, el procesador 4 recupera el identificador de usuario UID y el identificador DID1 de los datos DD1.

El procesador 4 obtiene (S40) a continuación, a partir de la clave madre RK grabada en la memoria segura M2, la clave derivada DK1 correspondiente a los datos cifrados CD1 grabados en la memoria no segura M1. En este ejemplo particular, el procesador 4 determina la clave derivada DK1 a partir de la clave madre RK utilizando el identificador de usuario UID y el identificador DID1 de los datos DD1, recuperados en la etapa de recuperación S38.

De manera ventajosa, por cuanto que el identificador de usuario UID y el identificador DID de datos son constantes, la clave derivada DK1 determinada a partir de la clave madre es siempre la misma, cualquiera que sea el momento en que se calcule la misma (entendiendo que la clave madre DK permanece, en este punto, inalterada en la memoria segura M2).

Siempre en este ejemplo, el procesador 4 graba la clave derivada DK1 en la memoria segura M2.

El procesador 4 descifra (S42) entonces, a partir de la clave derivada DK1, los datos cifrados CD1 del fichero CF1 a fin de recuperar los datos DD1 en su forma no cifrada. Estos datos DD1 son grabados (S44) en calidad de fichero no cifrado DF1 en la memoria segura M2.

En la forma de realización descrita en este punto, el descifrado S42 se realiza directamente en la memoria segura M2. En otras palabras, los datos DD1 suministrados en el descifrado S42 se graban directamente en la memoria segura M2 (sin efectuar grabación intermedia de los datos DD1 en otra memoria antes de la grabación S44 en la memoria segura M2).

Por otro lado, el procesador 4 determina (S46) la huella de resumen de los datos DD1 recuperados en S42 y luego verifica (S48) la integridad de estos datos DD1 en la memoria M2 comparando la huella de resumen determinada en la etapa de determinación S46 con la huella de resumen H1 grabada en el fichero de resumen HF en asociación con los datos DD1.

En caso de concordancia en la etapa de verificación S48, el procesador 4 pone en práctica la etapa de autorización S52. En caso contrario, el procesador 4 determina (S50) que los datos DD1 recuperados de la memoria segura M2 en la etapa S44 son inválidos, finalizando entonces el procedimiento.

En la etapa de autorización S52, el procesador 4 autoriza el acceso a los datos DD1 en la memoria segura M2 como respuesta a la petición de acceso RQ recibida en la etapa S32. En otras palabras, el procesador 4 únicamente autoriza el acceso a los datos DD1 recuperados de la memoria M2 en la etapa S44 si la verificación de integridad S48 se supera con éxito.

Así, la presente técnica permite ventajosamente acceder a los datos grabados en la memoria no segura M1 sin comprometer la confidencialidad de dichos datos. En el procedimiento, en ningún momento los datos se hallan presentes de forma no cifrada (en claro) en la memoria no segura M1. La invención permite además verificar de manera fiable que los datos a los que se accede a conveniencia en la memoria segura están íntegros.

Se describe a continuación, con referencia a la figura 5, un procedimiento de grabación segura puesto en práctica por el terminal 2 sobre los datos DD1, una vez terminado el acceso a dichos datos SD1.

Más concretamente, se supone ahora que, a consecuencia de la autorización concedida en la etapa de autorización S52, el usuario en cuestión ha accedido (S58) a los datos DD1 grabados en forma del fichero no cifrado DF1 en la memoria segura M2.

En el acceso S58 del usuario a los datos DD1 en la memoria M2, dichos datos DD1 son susceptibles de haber sido modificados (acceso de escritura). Así pues, a continuación del acceso S58, estos datos se señalan con DD1a y el fichero no cifrado que comprende dichos datos DD1a se señala con DF1a (como se representa en la figura 5).

En el curso de una etapa de determinación S60, el procesador 4 determina si se debe realizar un nuevo procedimiento de grabación segura de los datos DD1a presentes en la memoria segura M2. En caso afirmativo, el procesador 4 procede a las etapas S62-S72 que pasamos a describir. En el ejemplo de que se trata en este punto, el procesador 4 procede a las etapas S62-S72 cuando ha terminado el acceso a los datos DD1a (o, alternativamente, a la recepción de una petición del usuario).

En las etapas S62-72, el procesador 4 repite respectivamente las etapas de cifrado S8 de los datos, de grabación S10 de los datos, de determinación S12 de una huella de resumen, de grabación S14 de la huella de resumen, de grabación (o actualización) S16 de la huella de resumen general y de supresión (S18) de los datos (y, preferentemente, también de la clave derivada DK1), según están definidas anteriormente con referencia a la figura 3.

Más en particular, el módulo de cifrado ME cifra (S62), a partir de la clave derivada DK1, los datos DD1a de la memoria M2 a datos cifrados CD1a, siendo estos últimos grabados (S64) por el módulo de grabación MST1 en forma de un fichero cifrado CF1a en la memoria no segura M1. Nótese que, en la etapa de cifrado S62, el módulo de cifrado ME utiliza, en este punto, la clave derivada DK1 que previamente se ha grabado en la memoria segura M2 en el procedimiento de recuperación segura descrito previamente (etapa S40). Alternativamente, la clave derivada DK1

puede ser determinada nuevamente a partir de los identificadores UID y DID1.

El módulo de determinación MD determina (S66) además la huella de resumen, ahora señalada con H1a, del fichero no cifrado DF1a grabado en la memoria segura M2. El módulo de grabación MST2 graba (S68) entonces la huella de resumen H1a en el fichero HF en asociación con los datos DD1a (por ejemplo, con el identificador DID1).

Asimismo, el módulo de grabación MST3 actualiza (S70), en la memoria segura M2, la huella de resumen general GHV al objeto de que sea representativa del contenido del fichero de resumen HF que ahora comprende la huella de resumen H1a.

En el curso de la etapa de supresión S72, el módulo de supresión MS, por otro lado, suprime el fichero no cifrado DF1a y, preferentemente, la clave derivada DK1, de la memoria segura M2.

Así, de manera ventajosa, la invención permite consultar y, eventualmente, modificar datos grabados de forma cifrada en la memoria no segura del dispositivo de grabación de datos, y ello sin comprometer la confidencialidad de los datos en cuestión y asegurándose de que los datos a los que se accede están íntegros.

Se describe ahora, con referencia a la figura 6, una variante de realización a las etapas S62-S72.

Se supone asimismo, en este punto, que ha tenido lugar un acceso S58 a los datos DD1 en la memoria segura M2 según se ha descrito anteriormente con referencia a la figura 5.

De acuerdo con esta variante de realización, el procesador 4 determina a continuación, en la etapa S60, si se debe realizar un procedimiento de grabación segura de los datos DD1a presentes en la memoria segura M2, de igual manera a como se ha descrito anteriormente con referencia a la figura 5. En caso afirmativo, el procesador 4 pone en práctica la etapa de determinación S82.

En el curso de la etapa de determinación S82, el módulo de determinación ME determina la huella de resumen señalada con H1a de los datos DD1a grabados en la memoria segura M2, a continuación del acceso S58. En este ejemplo, el procesador 4 graba la huella de resumen H1a en la memoria segura M2.

El procesador 4 compara (S84) la huella de resumen H1a determinada en S82 con la huella de resumen H1 grabada en el fichero de resumen HF en asociación con los datos DD1, y determina (S84) si estas huellas de resumen H1a y H1 coinciden entre sí. En caso de no concordancia en la etapa S84, el procesador 4 pone en práctica la etapa de cifrado S62 y ejecuta las etapas S62-S72 según se han descrito anteriormente con referencia a la figura 5. En cambio, si el procesador 4 detecta en S84 que las huellas de resumen H1 y H1a coinciden entre sí, procede directamente a la etapa S72 tal y como está descrita anteriormente con referencia a la figura 5. En otras palabras, el procesador 4 únicamente repite las etapas de cifrado S62, de grabación S64 de los datos cifrados, de determinación S66 de una huella de resumen, de grabación S68 de dicha huella de resumen y de grabación (o actualización) S70 del valor de resumen general, tales y como se han definido anteriormente, si se detecta en S84 que los datos DD1a son diferentes de los datos DD1 (lo cual significa que los datos DD1 han sido modificados en el acceso S58).

Esta variante de realización es ventajosa en que permite evitar la repetición superflua de ciertas etapas del procedimiento de grabación segura a continuación del acceso a datos en la memoria segura del terminal. De ello resulta una ganancia de tiempo y de eficiencia, así como un ahorro de los recursos utilizados en el terminal.

Un experto en la materia comprenderá que las formas de realización y variantes descritas anteriormente tan sólo constituyen ejemplos no limitativos de puesta en práctica de la invención. En particular, un experto en la materia podrá contemplar cualquier combinación de las variantes y formas de realización descritas anteriormente con el fin de dar respuesta a una necesidad muy particular.

REIVINDICACIONES

1. Procedimiento de grabación segura de datos (DD1), puesto en práctica en un dispositivo de grabación de datos (2) que comprende una primera memoria no segura (M1) y una segunda memoria segura (M2), comprendiendo el procedimiento las siguientes etapas:

- obtención (S4), a partir de una clave madre (RK) grabada en la segunda memoria, de una clave derivada (DK1) correspondiente a los datos (DD1) grabados en la segunda memoria;

- cifrado (S8), a partir de la clave derivada, de los datos (DD1) suministrando datos cifrados (CD1);

- grabación (S10) de los datos cifrados (CD1) en la primera memoria (M1);

- determinación (S12) de una huella de resumen (H1) de dichos datos (DD1);

- grabación (S14) de dicha huella de resumen, en asociación con los datos (DD1), en un fichero de resumen (HF) grabado en la primera memoria;

- grabación (S16), en la segunda memoria, de una huella de resumen general (GHV) representativa del contenido del fichero de resumen (HF) que comprende dicha huella de resumen; y

- supresión (S18) de los datos (DD1) de la segunda memoria con posterioridad a dicha grabación (S10) de los datos cifrados (CD1) en la primera memoria.

2. Procedimiento según la reivindicación 1, en el que, después de su obtención (S4), la clave derivada es grabada (S6) en la segunda memoria (M2), comprendiendo además el procedimiento una etapa de supresión (S18) de la clave derivada de la segunda memoria tras el cifrado (S8) de dichos datos.

3. Procedimiento según una cualquiera de las reivindicaciones 1 ó 2, en el que la clave madre (RK) es generada de manera aleatoria en el dispositivo de grabación de datos.

4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, en el que, en la etapa de obtención (S4), la clave derivada (DK) se obtiene a partir:

- de un identificador de usuario (UID) representativo de un usuario del dispositivo de grabación de datos; y

- de un identificador (DID1) de los datos (DD1).

5. Procedimiento según la reivindicación 4, en el que, en dicha grabación (S10) de los datos cifrados (CD1), dichos datos cifrados se graban en la primera memoria (M1) en forma de un fichero cifrado (CF1) al que se atribuye un nombre de fichero (N1) que comprende el identificador de usuario (UID) y el identificador (DID1) de los datos (DD1).

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, que comprende, a continuación de dicha grabación (S14) de la huella de resumen en el fichero de resumen (HF), una grabación de una copia del fichero de resumen en una memoria segura de copia de seguridad del dispositivo de grabación de datos (2).

7. Procedimiento de recuperación segura de datos, puesto en práctica en un dispositivo de grabación de datos (2) que comprende una primera memoria no segura (M1) y una segunda memoria segura (M2), comprendiendo el procedimiento:

- una verificación (S30) de la integridad de un fichero de resumen (HF) grabado en la primera memoria, a partir de una huella de resumen general (GHV) grabada en la segunda memoria (M2); y

cuando el fichero de resumen se detecta como íntegro, el procedimiento comprende además, a la recepción de una petición de acceso (RQ) a datos (DD1), las siguientes etapas:

- obtención (S40), a partir de una clave madre (RK) grabada en la segunda memoria (M2), de una clave derivada (DK1) correspondiente a unos datos (CD1) grabados en la primera memoria;

- descifrado (S42), a partir de la clave derivada (DK1) obtenida, de los datos cifrados (CD1) a fin de recuperar dichos datos (DD1);

- grabación (S44) de dichos datos (DD1) en la segunda memoria (M2);

- determinación (S46) de la huella de resumen (H1) de dichos datos (DD1);

- verificación (S48) de la integridad de los datos (DD1) grabados en la segunda memoria comparando la huella de resumen (H1) determinada para los datos (DD1) con una huella de resumen (H1) grabada en el fichero de resumen (HF) en asociación con dichos datos (DD1); y

- autorización (S52) de un acceso a los datos (DD1) en la segunda memoria (M2) como respuesta a dicha petición de acceso (RQ), solamente si los datos se han determinado (S48) como íntegros.

8. Procedimiento según la reivindicación 7, que comprende una etapa de obtención (S38) de un identificador de usuario (UID) representativo de un usuario del dispositivo de grabación de datos y de un identificador (DID1) de los datos (DD1), en el que la clave derivada (DK1) se obtiene a partir de la clave madre (RK) utilizando el identificador de usuario y el identificador de los datos.

9. Procedimiento según una cualquiera de las reivindicaciones 7 u 8, que comprende, con posterioridad a un acceso (S58) a los datos (SD1), la ejecución de unas etapas de cifrado (S8) de los datos (DD1a) a datos cifrados (CD1a), de grabación (S10) de los datos cifrados (CD1a), de determinación (S12) de una huella de resumen (H1a), de grabación (S14) de la huella de resumen, de grabación (S16) de la huella de resumen general (GHV) y de supresión (S18) de los datos (DD1a), tales y como se han definido en el procedimiento de grabación segura según una cualquiera de las reivindicaciones 1 a 6.

10. Procedimiento según una cualquiera de las reivindicaciones 7 u 8, que comprende además, con posterioridad a un acceso (S58) del usuario a los datos (DD1) en la segunda memoria (M2), las siguientes etapas:

- determinación (S82) de una segunda huella de resumen (H1a) de dichos datos (DD1a) a continuación de dicho acceso; y

- comparación (S84) de dicha segunda huella de resumen (H1a) con la huella de resumen (H1) grabada en el fichero de resumen (HF) en asociación con los datos (DD1), con el fin de detectar si los datos (DD1) han sido modificados en dicho acceso;

en el que el procedimiento comprende la ejecución de unas etapas de cifrado (S8), de grabación (S10) de los datos cifrados, de determinación de una huella de resumen (S12), de grabación (S14) de dicha huella de resumen y de grabación (S16) de un valor de resumen general, tales y como se han definido en el procedimiento de grabación segura según una cualquiera de las reivindicaciones 1 a 6, únicamente si se detecta (S84) que los datos (DD1) han sido modificados en dicho acceso.

11. Programa de ordenador (PG) que incluye instrucciones para la ejecución de las etapas de un procedimiento de grabación segura de datos según una cualquiera de las reivindicaciones 1 a 6 o de un procedimiento de recuperación segura de datos según una cualquiera de las reivindicaciones 7 a 10, cuando dicho programa es ejecutado por un ordenador.

12. Dispositivo de grabación de datos (2) que comprende:

- una primera memoria no segura (M1);

- una segunda memoria segura (M2);

- un módulo de obtención (MO) configurado para obtener, a partir de una clave madre (RK) grabada en la segunda memoria, una clave derivada (DK) correspondiente a datos (DD1) grabados en la segunda memoria;

- un módulo de cifrado (ME) configurado para cifrar, a partir de la clave derivada, dichos datos (DD1) con objeto de suministrar datos cifrados (CD1);

- un primer módulo de grabación (MST1) configurado para grabar los datos cifrados (CD1) en la primera memoria;

- un módulo de determinación (MD) configurado para determinar una huella de resumen (H1) de dichos datos (DD1);

- un segundo módulo de grabación (MST2) configurado para grabar dicha huella de resumen (H1), en asociación con los datos (DD1), en un fichero de resumen (HF) grabado en la primera memoria (M1);

- un tercer módulo de grabación (MST3) configurado para grabar, en la segunda memoria (M2), una huella de resumen general (GHV) representativa del contenido del fichero de resumen (HF) que comprende dicha huella de resumen (H1); y

- un módulo de supresión (MS) configurado para suprimir los datos (DD1) de la segunda memoria (M2) con posterioridad a dicha grabación de los datos cifrados en la primera memoria (M1).

13. Dispositivo según la reivindicación 12, en el que:

- el módulo de obtención (MO) está configurado para grabar, en la segunda memoria, dicha clave derivada (DK) obtenida a partir de la clave madre (RK); y

- el módulo de supresión (MS) está configurado para suprimir la clave derivada grabada en la segunda memoria después del cifrado de dichos datos (DD1) por el módulo de cifrado (ME).

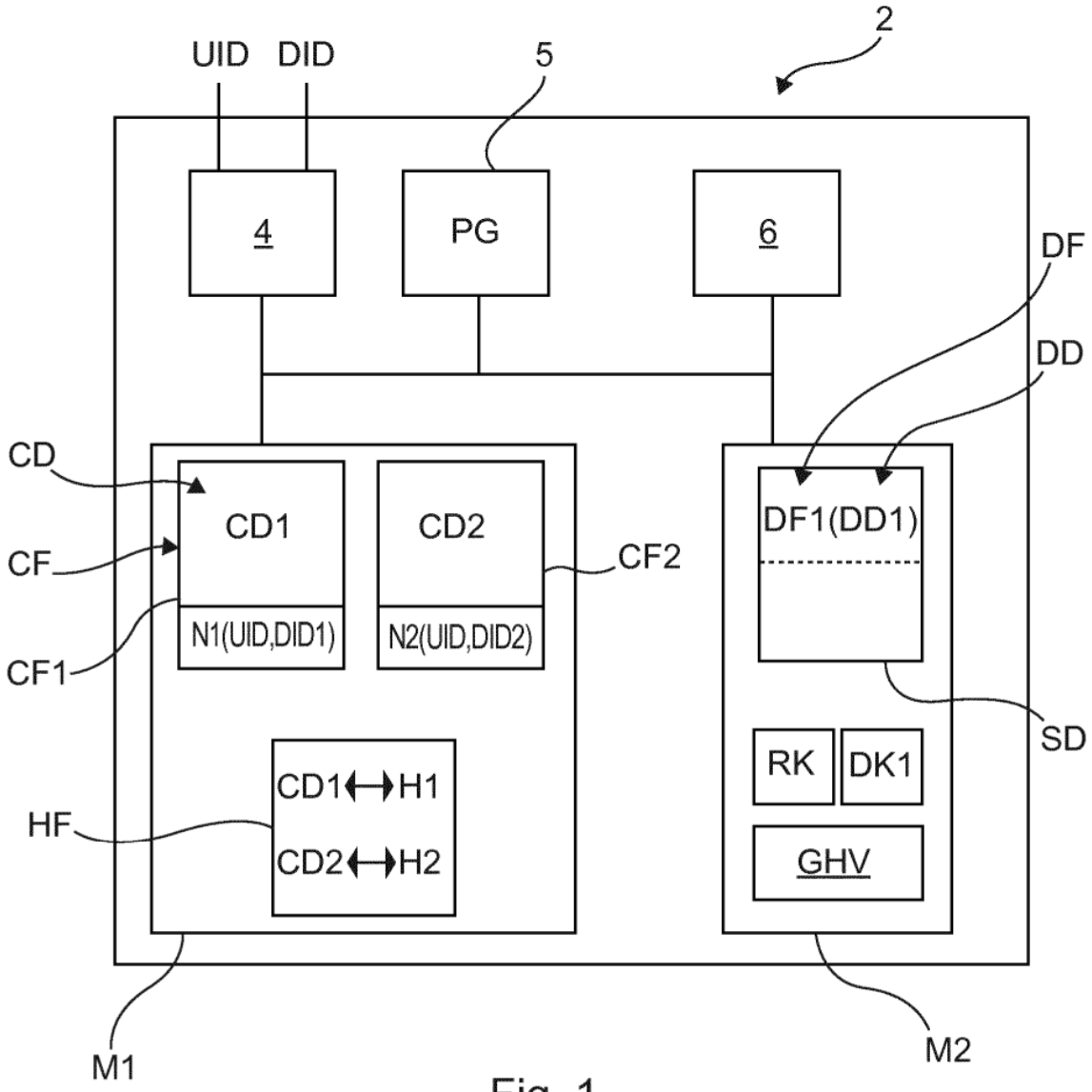
2
UID
DID
5
4
PG
6
DF
DD
CD
CF
CF1
CD1
CD2
CF2
N1(UID,DID1)
N2(UID,DID2)
DF1(DD1)
SD
RK
DK1
GHV
CD1↔H1
CD2↔H2
HF
M1
M2

Fig. 1

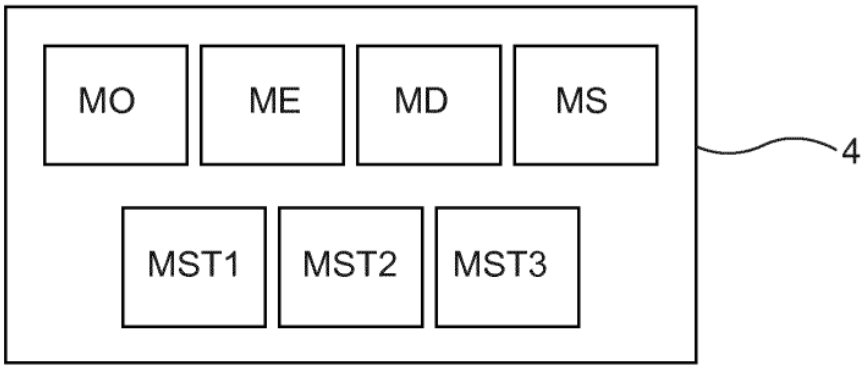
MO
ME
MD
MS
4
MST1
MST2
MST3

Fig. 2

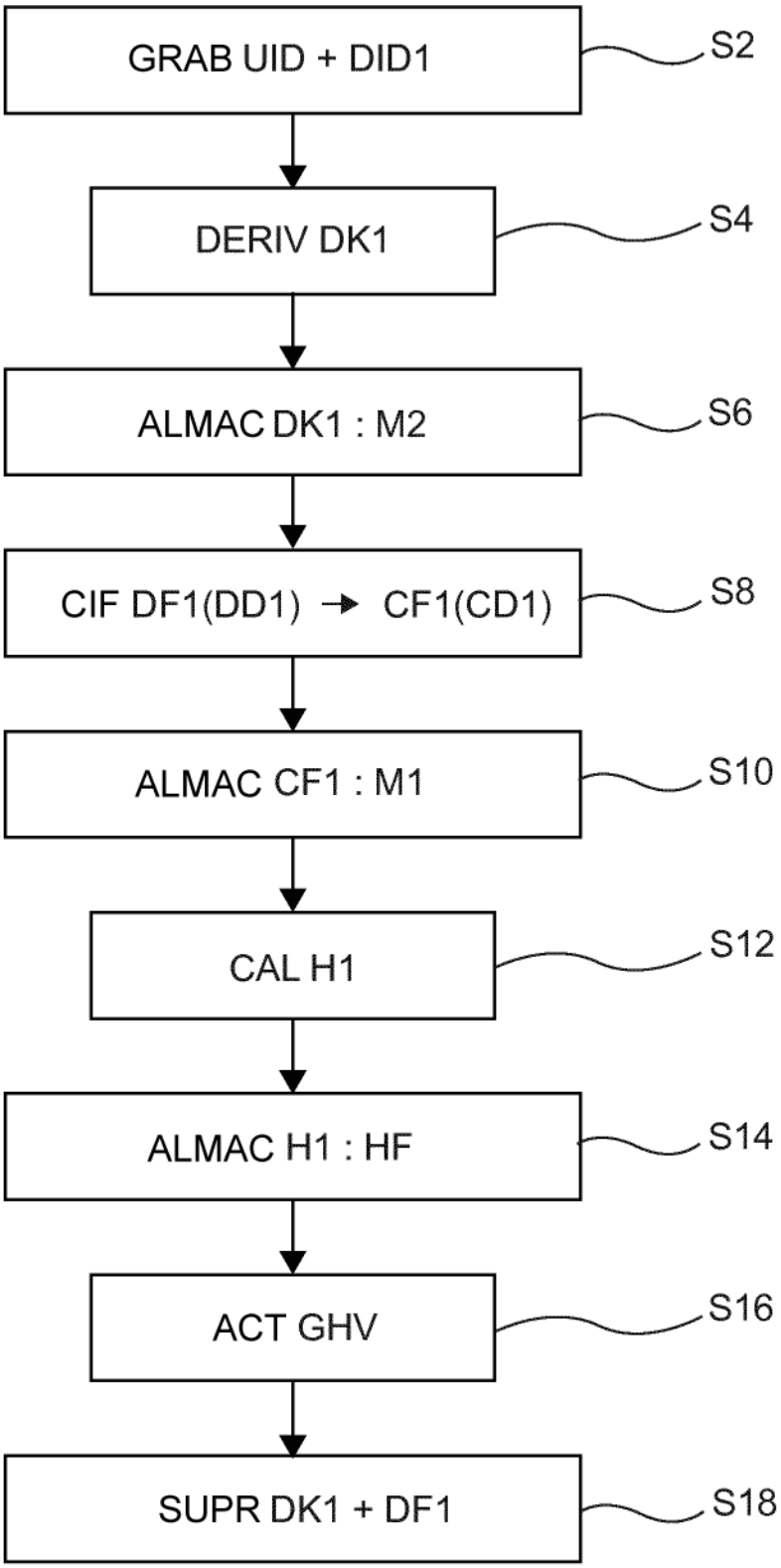
GRAB UID + DID1
S2
DERIV DK1
S4
ALMAC DK1 : M2
S6
CIF DF1(DD1) → CF1(CD1)
S8
ALMAC CF1 : M1
S10
CAL H1
S12
ALMAC H1 : HF
S14
ACT GHV
S16
SUPR DK1 + DF1
S18

Fig. 3

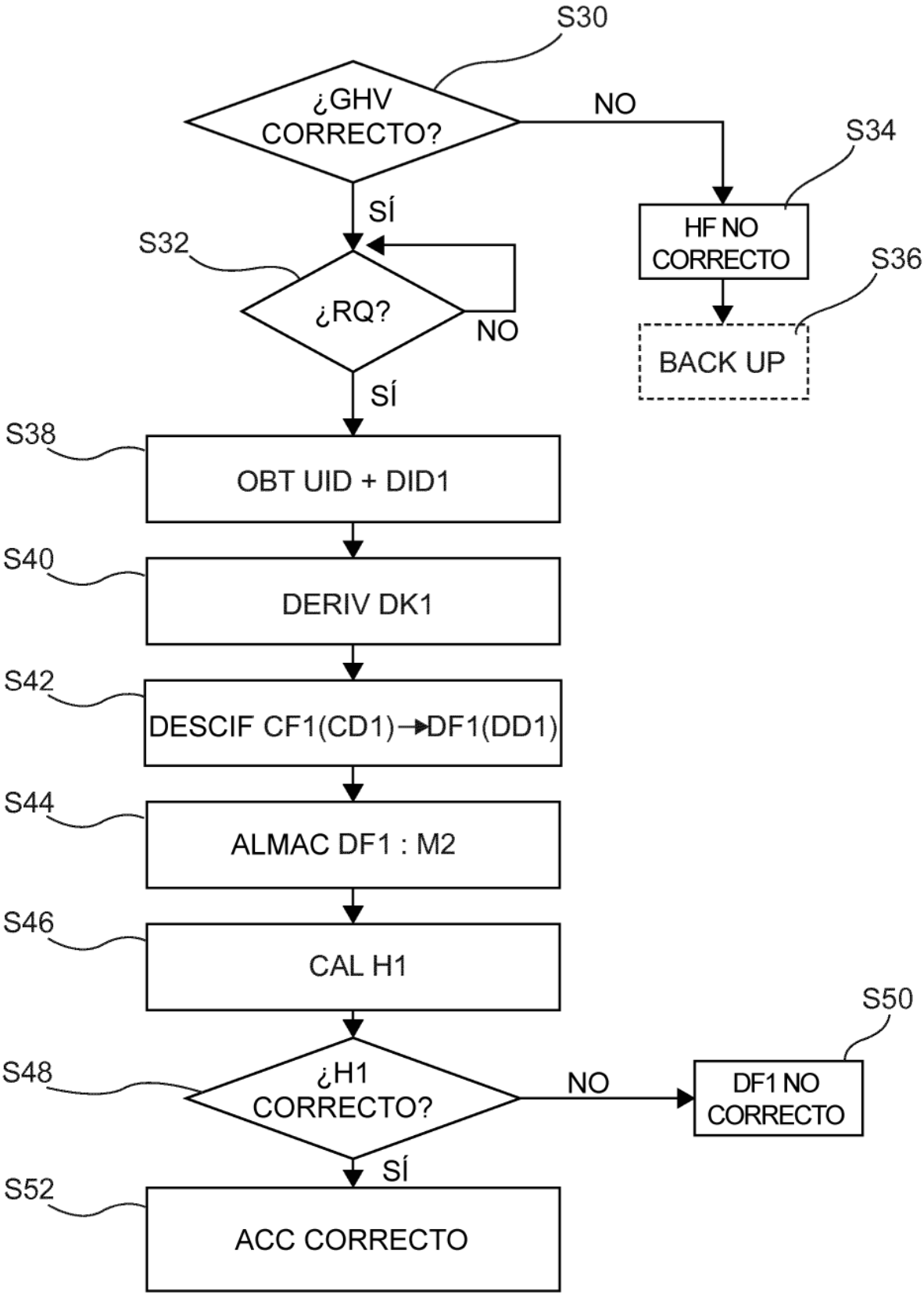
S30
¿GHV CORRECTO?
NO
S34
HF NO CORRECTO
S36
BACK UP
SÍ
S32
¿RQ?
NO
SÍ
S38
OBT UID + DID1
S40
DERIV DK1
S42
DESCIF CF1(CD1)→DF1(DD1)
S44
ALMAC DF1 : M2
S46
CAL H1
S50
S48
¿H1 CORRECTO?
NO
DF1 NO CORRECTO
SÍ
S52
ACC CORRECTO

Fig. 4

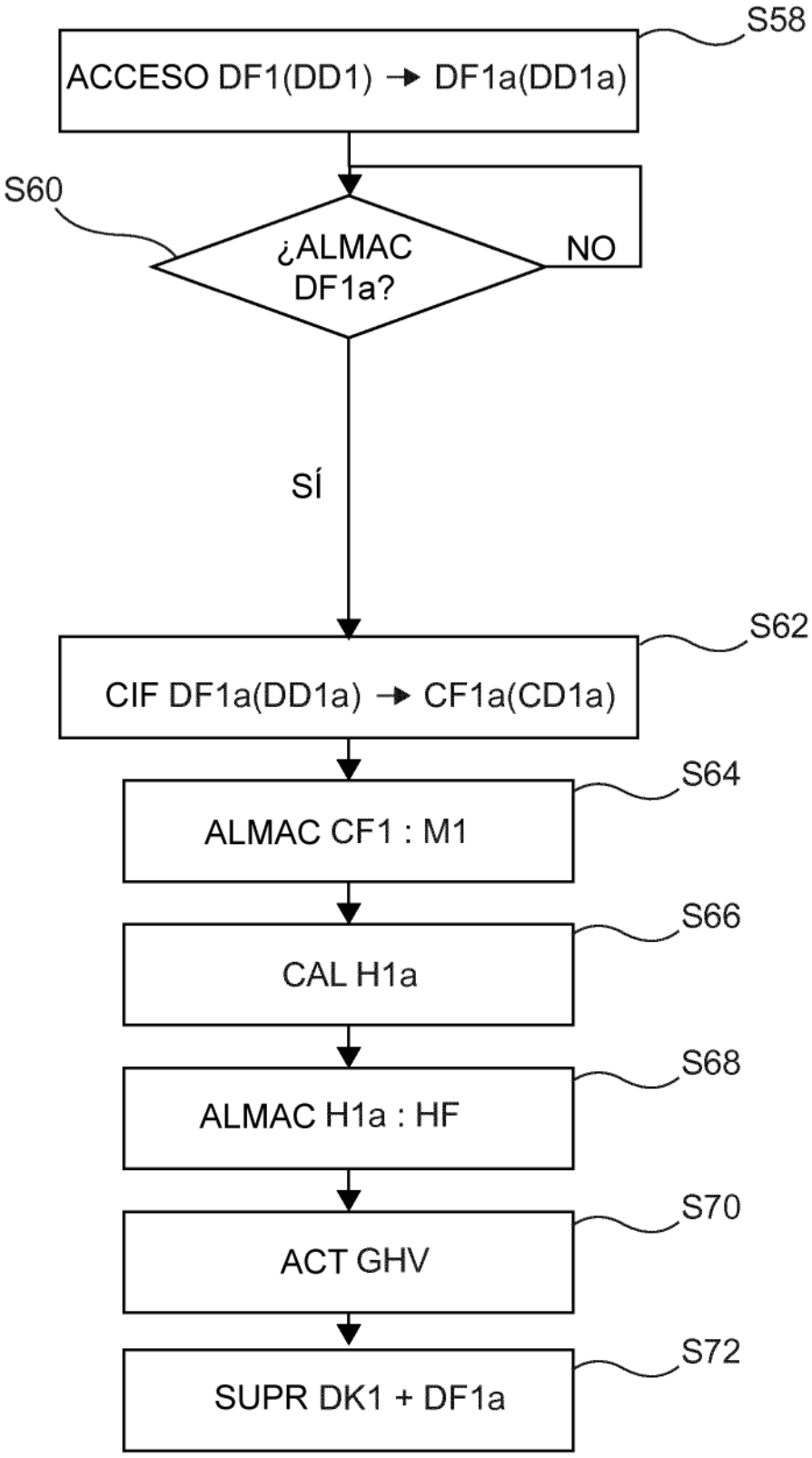
S58
ACCESO DF1(DD1) → DF1a(DD1a)
S60
¿ALMAC DF1a?
NO
SÍ
S62
CIF DF1a(DD1a) → CF1a(CD1a)
S64
ALMAC CF1 : M1
S66
CAL H1a
S68
ALMAC H1a : HF
S70
ACT GHV
S72
SUPR DK1 + DF1a

Fig. 5

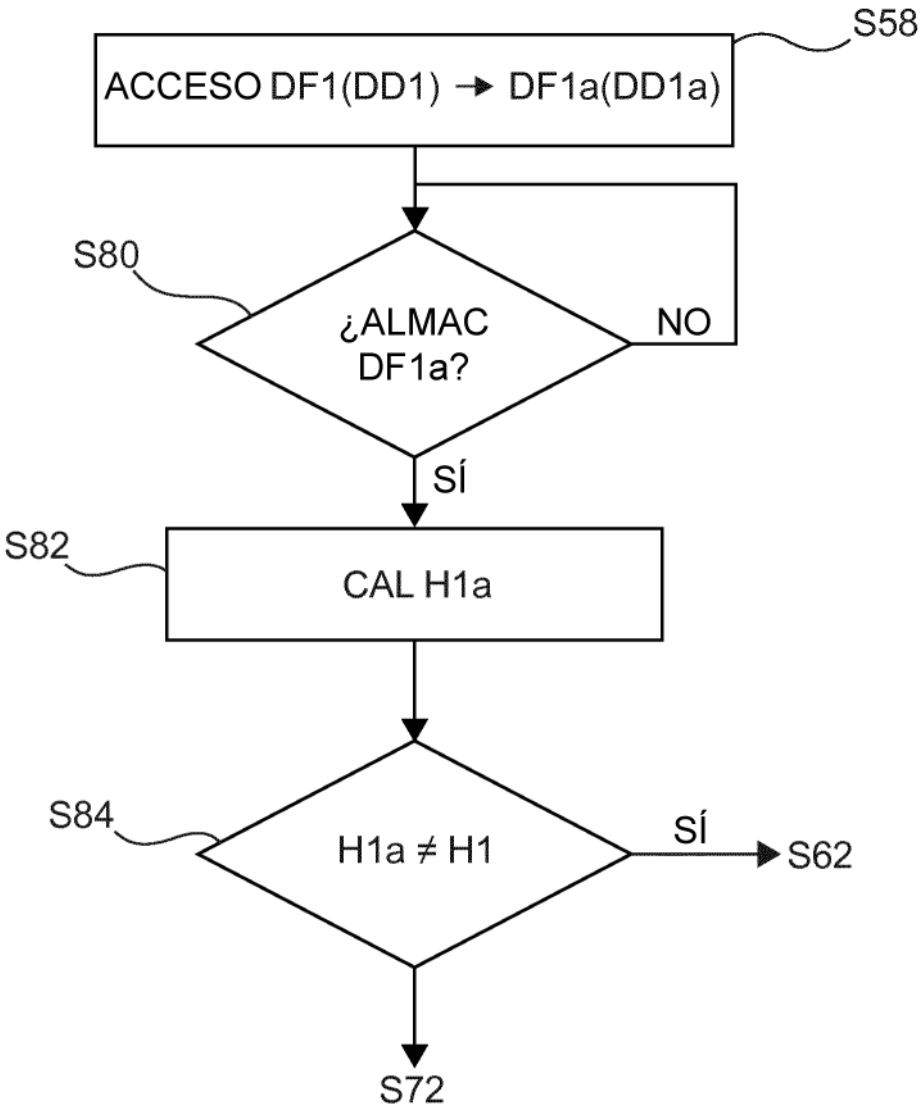
S58
ACCESO DF1(DD1) → DF1a(DD1a)
S80
¿ALMAC DF1a?
NO
SÍ
S82
CAL H1a
S84
H1a ≠ H1
SÍ
S62
S72

Fig. 6