(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 756 448**

(51) Int. CI.:

A47J 36/32 (2006.01)
H04L 9/32 (2006.01)
G06F 21/78 (2013.01)
G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.05.2014 E 14167280 (8)**

(97) Fecha y número de publicación de la concesión europea: **23.10.2019 EP 2801928**

(54) Título: **Procedimiento para el almacenamiento protegido por copia de informaciones en un soporte de datos**

(30) Prioridad:

08.05.2013 DE 102013104735

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.04.2020

(73) Titular/es:

VORWERK & CO. INTERHOLDING GMBH (100.0%)
Mühlenweg 17-37
42275 Wuppertal, DE

(72) Inventor/es:

GREIVE, VOLKER

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento para el almacenamiento protegido por copia de informaciones en un soporte de datos

La invención se refiere a un procedimiento para el almacenamiento protegido con copia de una información, constituida, por datos digitales, en un soporte de datos y para la lectura de la información desde el soporte de datos, en donde el soporte de datos presenta una identificación digital individual, en donde se forma un signatura que comprende la identificación individual, en donde la información posee al menos componentes de información que sólo pueden ser procesados por una instalación electrónica de procesamiento de datos cuando la identificación digital individual y la signatura están en una relación predeterminada entre sí.

Un procedimiento del tipo designado anteriormente se describe en el documento DE 102009018941 A1. Para el control de acceso a un sistema de ficheros codificado de un medio de memoria debe utilizarse allí una identificación individual el elemento de memoria. Cada elemento de memoria fabricado tiene un número de serie asociado individualmente al elemento de memoria y, por lo tanto, predeterminado sólo una vez. En el estado de la técnica, a partir de este número de serie y una referencia a una clave de un grupo de claves se forma una clave parcial. El acceso al sistema de ficheros por medio de una Estación de Acceso de Medios Seguros sólo debe estar permitido cuando la identificación posee una relación correcta con la clave. Una copia de la clave en otro medio de memoria tiene, por lo tanto, como consecuencia que se desvía el acceso. La clave parcial o una identificación obtenida a partir de ella por medio de una función Hash deben firmarse con una clave personal, por ejemplo basad en un cripto-sistema asimétrico, por ejemplo basado en RSA-2048.

El documento US 2006/0064488 A1 describe un procedimiento para la comercialización de software y un sistema utilizado en este caso para la gestión de derechos digitales. El documento EP 2573632 A1 describe un aparato electrodoméstico, al que se puede transferir un programa de aparato electrodoméstico. El programa está equipado con una identificación.

Se conocen a partir del documento DE 102007059236 A1 aparatos electrodomésticos de motor eléctrico, en particular máquinas de cocina. Los aparatos electrodomésticos que pueden ser accionados con motor eléctrico que pertenecen al estado de la técnica están en condiciones de trabajar según un programa depositado en una memoria de programa, en donde el programa contiene etapas de programa que se suceden en el tiempo y las etapas del programa se diferencian por diferentes parámetros del procedimiento, como temperatura de procesamiento o número de revoluciones de un mecanismo de agitación o duración de una etapa de proceso. Los dos de control del proceso correspondientes se almacenan en una instalación de memoria de un circuito integrado de semiconductores.

La invención tiene el cometido de indicar medidas con las que se puede abastecer un aparato electrodoméstico de motor eléctrico con datos de control de proceso y/o con datos reproducibles con una interfaz de hombre-máquina, en donde debe asegurarse al mismo tiempo que sólo se emplean datos originales.

El cometido se soluciona por medio de la invención indicada en las reivindicaciones.

Con el procedimiento según la invención se preparan informaciones constituidas por datos digitales en un soporte de datos. La autenticidad de estas informaciones digitales se puede verificar utilizando la identificación firmada individual. Sólo son procesadas por la instalación electrónica de procesamiento de datos, es decir, leídas y reconocidas, cuando la identificación digital individual, en la que se puede tratar de un número de serie único, y la signatura generada en la fabricación del soporte de datos o bien durante el almacenamiento de los datos digitales sobre el soporte de datos están en una relación predeterminada entre sí. La relación puede estar configurada como cifrado. Se puede tratar de una relación de sumas de prueba de la identificación individual del soporte de datos y de la signatura. La signatura digital se puede generar de manera conocida utilizando una función Hash, en donde previamente se escribe la identificación digital individual, es decir, el número de serie del soporte de datos, especialmente de una unidad-USB, en la que se escribe el fichero que lleva la información o en un fichero separado, pero que pertenece al mismo sistema de ficheros. Este fichero firmado de manera conocida con una clave privada se almacena entonces en el soporte de datos. Se contemplan aquí, por ejemplo, los cripto-sistemas asimétricos mencionados al principio. La instalación electrónica de procesamiento de datos dispuesta en el aparato electrodoméstico de motor eléctrico está programada de tal manera que sólo acepta el soporte de datos o bien las informaciones almacenadas en él cuando se puede verificar la signatura. Si se utiliza un cripto-sistema, que está constituido por una clave privada y una clave pública, entonces se puede verificarla signatura con la ayuda de la clave pública. En esta variante preferida, se establece la relación a través de la utilización de la clave pública y la comparación de los números de serie almacenados en el fichero con los números de serie reales del soporte de datos. En este caso, una vez realizada la verificación con éxito, se compara la identificación digital individual almacenada en el fichero, es decir, especialmente los números de serie con los números de serie del propio soporte de datos, y se verifica si los dos números son idénticos. Si los números de serie no coinciden o bien no se puede verificar la signatura como consecuencia de una manipulación en la información almacenada en el soporte de datos,

se rechaza el procesamiento de la información depositada en el soporte de datos digital. Según la invención, sin embargo, en la signatura no se realiza ninguna codificación, en el sentido de que la información pueda leerse sólo utilizando una clave adecuada. Según la invención, más bien está previsto que la información posea al menos componentes de la información que pueden ser procesados, es decir, leídos y evaluados por una segunda instalación electrónica de procesamiento de datos, es decir, por ejemplo un PC habitual u otro aparato de visualización de datos, especialmente puedan reproducirse en una interfaz hombre-máquina, aunque la signatura y la identificación no estén en relación predeterminada entre sí, es decir, una verificación errónea o bien el número de serie almacenado en el fichero no coincide con el número de serie del soporte de datos. Las informaciones almacenadas en el soporte de datos pueden presentar componentes de la información cualitativamente diferentes entre sí. De esta manera, las informaciones pueden presentar componentes de la información en forma de ficheros de texto, ficheros de audio, ficheros de vídeo o ficheros de imágenes. Estos datos, que pueden ser registrados por un usuario, pueden ser emitidos a través de diferentes interfaces hombre-máquina; por ejemplo, los ficheros de texto y los ficheros de datos se pueden representar en una pantalla de un PC. Los datos respectivos pueden estar almacenados en formado-PFD, en formato-PTF, en formato-HTML, en formato-XML, en formato SQLite o en otro formato, especialmente utilizando un “concepto mark-up-language”, pudiendo ser almacenado el número de serie en componentes no representables de los ficheros. Pero el número de serie se puede almacenar también en un fichero separado, igualmente almacenado sobre el soporte de datos. Al menos este fichero se firma. Por lo demás, las informaciones pueden contener datos de control de la máquina. Los datos de control de la máquina son con preferencia datos de control de proceso, que contienen parámetros del proceso en un protocolo apropiado, pudiendo ser los parámetros de proceso, entre otros, la duración de un proceso, la temperatura de una etapa del proceso y/o el número de revoluciones de un agitador. Estos datos de control de procesos pueden estar almacenados también codificados en el soporte de datos, de manera que no pueden ser procesados por una segunda instalación electrónica de procesamiento de datos.

La invención se refiere, además, a un sistema para realizar el procedimiento, que consta de un soporte de datos, sobre el que está almacenada una información que consta de datos digitales, presentando el soporte de datos una identificación digital individual, que está almacenada como la información en el soporte de datos, siendo firmada, sin embargo, la identificación individual. El sistema presenta, además, una instalación electrónica de procesamiento de datos, que está programada para que rechace el procesamiento de los datos digitales depositados en el soporte de datos cuando la identificación digital individual y la signatura no están en una relación predeterminada entre sí, es decir, cuando o bien una signatura no es verificable o la identificación digital almacenada en el soporte de datos no coincide con la identificación digital real de la memoria de datos. Según la invención, la instalación electrónica de procesamiento de datos es componente de un aparato electrodoméstico que puede ser accionado con motor eléctrico, especialmente un aparato de cocina y especialmente preferido es parte de un dispositivo para la preparación de comidas según una receta predeterminada, estando almacenada la receta en el soporte de datos como información.

La invención se refiere, además, a un aparato electrodoméstico que puede ser accionado con motor eléctrico, especialmente una máquina de cocina, que presenta una instalación electrónica de procesamiento de datos, que está programada pata que esté en condiciones de leer datos desde un soporte de datos que se puede conectar a través de una interfaz con la instalación electrónica de procesamiento de datos, estando programada la instalación electrónica de procesamiento de datos para verificar la signatura de los datos digitales depositados en el soporte de datos digitales y en el caso de verificación con éxito para comparar un valor comprendido por la signatura, almacenado en el soporte de datos para una identificación digital individual con la identificación digital real del soporte de datos. El aparato electrodoméstico está instalado, además, de manera que rechaza el procesamiento de la información cuando o bien falla la verificación de la signatura o la identificación digital individual almacenada no coincide con la identificación digital individual real del soporte de datos. El aparato electrodoméstico según la invención está en condiciones, además, de realizar un proceso de procesamiento que consta de varias etapas sucesivas, especialmente un proceso de preparación de comida, donde los datos de proceso son datos de control de proceso almacenados en el soporte de datos digitales.

La invención se refiere, además, a un circuito integrado, especialmente en forma de un medio de memoria con una memoria integrada y con un controlador integrado, en donde datos digitales están almacenados en la memoria integrada y el medio de memoria presenta una identificación digital individual. Es esencial que la información almacenada en el medio de memoria sea una receta de procesamiento, que se puede representar en una interfaz hombre-máquina, por ejemplo una pantalla en forma de texto y/o de imágenes y/o comprende datos de control de proceso ejecutable por un aparato electrodoméstico. En la memoria integrada está depositada en forma de datos digitales una signatura, que es verificable por una instalación electrónica de procesamiento de datos del tipo designado anteriormente.

A continuación se explica un ejemplo de realización con la ayuda del dibujo adjunto.

El dibujo muestra en forma de un diagrama de bloques el ciclo de un procedimiento para depositar una información que consta de datos digitales y la lectura de esta información así como un sistema que procesa según este procedimiento.

En el lugar E de la figura se representa una máquina de cocina accionada eléctricamente, como se describe en el documento DE 102007059236 A1. El contenido del documento DE 102007059236 A1 se cita con la finalidad de incluir características en reivindicaciones de la presente invención.

El número de referencia 11 caracteriza una instalación electrónica de procesamiento de datos integrada en la máquina electrónica de cocina. Esta primera instalación electrónica de procesamiento de datos 11 puede estar configurada por un microcontrolador. La máquina de cocina posee una interfaz no representada, con la que se puede conectar operativamente un medio externo de memoria con la instalación electrónica de procesamiento de datos 11.

Con el número de referencia 1 se designa una unidad-USB habitual, que posee una interfaz en serie universal, con la que se puede llevar la unidad-USB 1 a una conexión de transmisión de datos con la instalación electrónica de procesamiento de datos 11 de la máquina de cocina o bien con una segunda instalación electrónica de procesamiento de datos 12 en forma de un PC habitual.

El soporte de datos digitales 1 posee un medio de memoria con una memoria integrada y un controlador integrado. En ella se deposita una identificación 2 individual en forma de un número de serie universal, es decir, único. Este número de serie se identifica en la figura 1 simbólicamente con el número de referencia 2.

El número de referencia 3 designa un fichero, que presenta informaciones digitales 4 y 5. En las informaciones digitales 4 se puede tratar de informaciones que se pueden representar en un aparato de visualización de datos de un PC 12, por ejemplo textos o imágenes, pero también dicheros de audio o de video. Tales ficheros, por ejemplo ficheros PDF, RTF, HTML, XML, SQLite no sólo contienen puras informaciones, sino informaciones complementarias, que están almacenadas allí como etiquetas o metadatos individuales. Igualmente como información no visible o bien no detectable por los sentidos se almacena en el mismo fichero 3 o en un fichero que pertenece al mismo sistema de ficheros un valor que corresponde al número de serie 2 del soporte de datos 1. Además, el fichero 3, que puede estar constituido también por un conjunto de varios ficheros, puede llevar datos de control de la máquina 5, en los que se trata de datos de control de proceso, con los que la instalación electrónica de procesamiento de datos 11 de la máquina de cocina puede ejecutar allí un programa de preparación de comida, conteniendo los datos de control de proceso 5 al menos la duración de una etapa individual de procesamiento, la temperatura de la etapa de procesamiento y un número de revoluciones del agitador.

En el lugar designado con A del diagrama de flujo se crea de esta manera un fichero o un conjunto de varios ficheros 3, que contiene la identificación 2 individual, una receta de procedimiento 4 en texto claro y datos de control de la máquina 5 asociados de manera óptima.

En el lugar designado con B se crea con una función-HASH 8 un número de prueba de muchos dígitos que identifica la individualidad del dichero o bien del conjunto de varios ficheros 3. El valor-HASH se puede generar, por ejemplo, utilizando el Message Digest Algorythm 2 (MD 2) o, en cambio, también algoritmos similares, por ejemplo MD 4, MD 5 o SHA 256 etc. Con preferencia, se utiliza el algoritmo SHA 256, puesto que se considera como el mejor compromiso de seguridad y velocidad de procesamiento.

En el lugar C del plan de flujo se representa una pareja de claves asimétricas, que contiene una clave pública 6 y una clave privada 7. Las dos claves 6, 7 tienen la propiedad de que ficheros codificados con una clave pública 6 sólo pueden ser descodificados con la clave privada 7 correspondiente - y utilizando de la invención - se pueden firmar ficheros con la clave privada, siendo verificable la signatura sólo utilizando la clave pública 6. La pareja de claves respectivas se puede generar de manera conocida según el algoritmo-RSA con número suficiente de bits.

Utilizando la clave privada 7 se firma el valor-HASH 8 generado en el lugar B. La signatura 9 resultante en este caso contiene al menos el valor del número de serie 2 individual. Pero en el ejemplo de realización, la signatura 9 se extiende sobre todo el fichero 3, que comprende la información 4, 5 y la identificación digital 2 individual.

El lugar D simboliza que la signatura digital 9 se ha añadido como certificado 10 en el fichero 3 o en el conjunto de varios ficheros 3.

Este fichero 3 o bien el sistema de ficheros 3 se almacena ahora sobre el soporte de datos digitales 1, del que se ha tomado la identificación digital 2 individual.

Si debe almacenarse la información 4, 5 también en uno, especialmente en otros varios soportes de datos, deben generarse signaturas individuales 9 respectivas, que se almacenan junto con las informaciones 4, 5 en el soporte de datos 1 respectivo.

Si se modifican las informaciones 4, 5 almacenadas en el soporte de datos 1, no se puede verificar por la primera instalación electrónica de procesamiento de datos 11 la signatura 9 o bien el certificado 10. La verificación se realiza

utilizando la clave pública 6, que se utiliza por un programa, que se implementa en la instalación electrónica de procesamiento de datos 11 en la máquina de cocina. La verificación 13 se realiza en primer lugar a través de la verificación de la signatura 9 con la ayuda de la clave pública 6 y a continuación de la verificación del número de serie 2 depositado en el fichero 3 con el número de serie real 2 del soporte de datos 1. Si se ha copiado el fichero 3 o las informaciones que pertenecen a un conjunto de ficheros 3 en otro soporte de datos, que posee otro número de serie 2, entonces se deriva el procesamiento de las informaciones 4, 5 desde la primera instalación electrónica de procesamiento de datos 11, por que los números de serie 2 no coinciden. Lo mismo se aplica para datos manipulados, puesto que entonces la signatura 9 no se puede verificar.

No obstante, las informaciones 4 perceptibles por los sentidos pueden ser procesadas, sin embargo, por un PC habitual, que representa una segunda instalación electrónica de procesamiento de datos 12, es decir, que pueden ser mostradas o bien detectables por los sentidos.

De esta manera, es posible copiar con frecuencia opcional, por ejemplo, recetas legibles para la preparación de comidas. Las copias se pueden leer y representar entonces por un PC 12 opcional. Pero no se pueden utilizar para la preparación de comidas por medio de la máquina de cocina, que presenta la primera instalación electrónica de procesamiento de datos 11.

Lista de signos de referencia:

1	Unidad USB
2	Identificación
3	Fichero
4	Información
5	Información
6	Clave pública
7	Clave privada
8	Valor-HASH
9	Signatura digital
10	Máquina de cocina
11	Primera instalación electrónica de procesamiento de datos
12	Segunda instalación electrónica de procesamiento de datos
13	Verificación

REIVINDICACIONES

1. Procedimiento para el almacenamiento de una información (4, 5) que consta de datos digitales sobre un soporte de datos (1) y lectura de la información desde el soporte de datos (1), en el que el soporte de datos (1) presenta una identificación digital (2) individual, en el que durante el almacenamiento se deposita una signatura (10) generada a partir de la identificación (2) individual, en el que la información posee datos de control de la máquina (5), en el que durante la lectura se verifica la signatura (10) a través de una primera instalación electrónica de procesamiento de datos (11), y los datos de control de la máquina (5) sólo se pueden procesar por una primera instalación electrónica de procesamiento de datos (11) cuando la identificación digital (2) individual y la signatura (10) están en una relación predeterminada entre sí, en el que la primera instalación electrónica de procesamiento de datos (11) es parte de una máquina de cocina accionable con motor eléctrico para la preparación de comida, en el que los datos de control de la máquina (5) comprenden parámetros de procedimiento como temperatura, número de revoluciones del mecanismo de agitación así como tiempos de etapas de procesamiento sucesivas, y en el que la información posee una receta de preparación de comida (4) reproducible en forma de texto y/o de imagen, que puede ser reproducida por una segunda instalación electrónica de procesamiento de datos (12) por una interfaz hombre-máquina cuando la signatura (10) y la identificación (2) no están en la relación predeterminada entre sí, y que está asociada a los datos de control de la máquina (5).

2. Procedimiento según la reivindicación 1, caracterizado por que para la generación de la signatura (10) se utiliza una pareja de claves asimétricas, que están constituidas por una clave privada y una clave pública, en el que la signatura se genera utilizando la clave privada, y se realiza una verificación utilizando la clave pública por la primera instalación electrónica de procesamiento de datos (11).

3. Procedimiento según la reivindicación 2, caracterizado por que para la generación de la signatura (10) o bien se codifica la información (4, 5) completada con la identificación (2) individual con la clave privada o se codifica un valor-HASH formado a partir de ello con la clave privada.

4. Procedimiento según una de las reivindicaciones 2 ó 3, caracterizado por que la signatura (10) es componente de un fichero que presenta las informaciones (4, 5) y la identificación (2) individual, almacenado en el soporte de datos (1) o es un fichero separado almacenado en el soporte de datos (1).

5. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la información (4, 5) está almacenada como fichero "mark-up-language", especialmente en un formato PDF, SQLite, RTF, HTML, JPG, TIF o XML en el soporte de datos (1).

6. Procedimiento según una de las reivindicaciones anteriores, caracterizado por que la identificación individual es un número de serie especialmente predeterminado una vez (número de serie único).

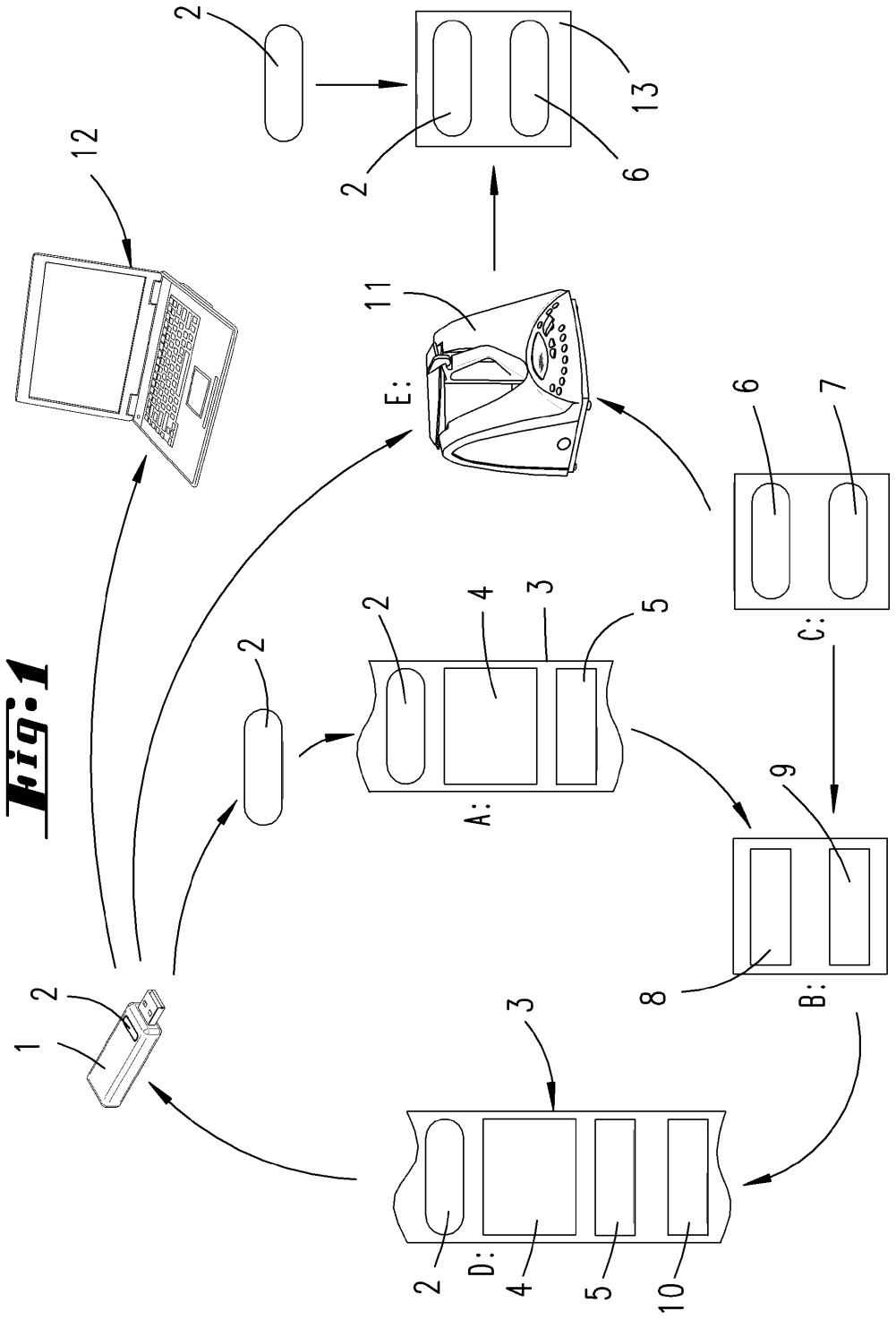
7. Sistema para realizar especialmente un procedimiento según una de las reivindicaciones anteriores, que comprende al menos un soporte de datos (1), en el que está almacenada una información (4, 5) constituida de datos digitales, en el que el soporte de datos (1) presenta una identificación digital (2) individual, en el que una signatura generada a partir de la identificación (2) individual está almacenada en el soporte de datos (1), en el que la información posee datos de control de la máquina (5), y una primera instalación electrónica de procesamiento de datos (11) está configurada para verificar la signatura (10), y para procesar los datos de control de la máquina (5) sólo cuando la identificación digital (2) individual y la signatura (10) están en una relación predeterminada entre sí, en el que la primera instalación de procesamiento de datos (11) es parte de una máquina de cocina accionable con motor eléctrico para la preparación de comida, en el que los datos de control de la máquina (5) comprenden parámetros de procedimiento como temperatura, número de revolucione del mecanismo de agitación así como tiempos de etapas de procesamiento sucesivas, y en el que la información posee una receta de preparación de comida reproducible en forma de texto y/o de imagen, que puede ser reproducida por una segunda instalación electrónica de procesamiento de datos (12) también desde una interfaz hombre-máquina, cuando la signatura (10) y la identificación (2) no están en la relación predeterminada entre sí y que está asociada a los datos de control de la máquina (5).

8. Sistema según la reivindicación 7, caracterizado por que el soporte de datos es una unidad-USB.

9. Circuito integrado de semiconductores con un circuito de control para la comunicación en serie o paralela con una primera o una segunda instalación de procesamiento de datos (11, 12) y con una instalación de memoria, cuyo circuito de semiconductores presenta una identificación digital (2) individual, y sobre cuya instalación de memoria una información (4, 5) constituida de datos digitales presenta los datos de control de la máquina (5) así como está almacenada una signatura (10) generada a partir de la identificación digital (2), en el que la identificación digital (2) individual y la signatura (10) están en una relación predeterminada entre sí, en el que los datos de control de la máquina (5) comprenden parámetros de procedimiento como temperatura, número de revoluciones del mecanismo de agitación así como tiempos de etapas sucesivas de procesamiento para una máquina de cocina accionable

eléctricamente para la preparación de comida, en el que la información posee, además, una receta de preparación de comida asociada a los datos de control de la máquina (5), reproducible en forma de texto y/o de imagen.

10. Máquina de cocina accionable con motor eléctrico, que presenta una instalación electrónica de procesamiento de datos (11), que está instalada para leer información (4, 5) y una signatura (10), que está almacenada según una de las reivindicaciones de procedimiento anteriores en un soporte de datos (1), que presenta una identificación digital (2) individual, para verificar la signatura (10), y para procesar datos de control de proceso (5), que son componentes de esta información (4, 5) sólo cuando la identificación digital (2) individual y la signatura (10) están en una relación predeterminada entre sí.



Fig·1