

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 673 561**

51 Int. Cl.:

**G06F 21/55** (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **31.08.2016** E 16186496 (2)

97 Fecha y número de publicación de la concesión europea: **14.03.2018** EP 3139296

54 Título: **Sistema informático de gestión segura de informaciones digitales**

30 Prioridad:

**07.09.2015 FR 1558289**

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

**22.06.2018**

73 Titular/es:

**DOCAPOST DPS (100.0%)  
10/12 Avenue Charles de Gaulle  
94220 Charenton le Pont, FR**

72 Inventor/es:

**LAURENT, ANTOINE**

74 Agente/Representante:

**SALVA FERRER, Joan**

**ES 2 673 561 T3**

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

## DESCRIPCIÓN

Sistema informático de gestión segura de informaciones digitales

- 5 **[0001]** La presente invención se refiere a un sistema informático de gestión segura de informaciones digitales utilizable en el campo del archivo digital.
- [0002]** En particular, la invención se refiere a tal sistema informático de gestión segura de informaciones digitales que aplican la trazabilidad con valor probatorio de estas informaciones digitales.
- 10 **[0003]** Tal sistema comprende:
- unos medios de producción de informaciones digitales;
  - unos medios de conservación de informaciones digitales;
  - 15 - unos medios de difusión y de consumo de informaciones digitales;
  - unos medios de trazabilidad de informaciones numéricas que constan de un registro de eventos relativos a unas informaciones digitales y unos medios de detección aptos para detectar cada evento relativo a cada información digital conservada en los medios de conservación, para registrar este evento en el registro de eventos.
- 20 **[0004]** Se conoce en el estado de la técnica, la utilización de unos sistemas informáticos de gestión segura de informaciones digitales que permiten aplicar la trazabilidad con valor probatorio de estas informaciones digitales.
- [0005]** En particular, estos sistemas aseguran la gestión segura de informaciones digitales durante diferentes fases de vida de estas informaciones que comprenden especialmente una fase de producción, una fase de conservación y una fase de consumo.
- 25 **[0006]** El conjunto de estas fases forma entonces un ciclo de vida de la información digital correspondiente.
- [0007]** Los sistemas de gestión permiten además conservar de manera segura las informaciones digitales y trazar cualquier evento relativo a las informaciones numéricas conservadas.
- 30 **[0008]** Cada información digital se presenta, por ejemplo, bajo la forma de un documento electrónico o de cualquier otro fichero informático cuya conservación a largo plazo es necesaria.
- 35 **[0009]** Se concibe entonces que los sistemas informáticos de gestión encuentran especialmente su aplicación en el campo del archivo numérico de los documentos electrónicos.
- [0010]** Así, cada evento relativo a un documento electrónico comprende, por ejemplo, la apertura, la modificación, la duplicación o la supresión de este documento electrónico.
- 40 **[0011]** La trazabilidad de las informaciones digitales asegurada por estos sistemas debe responder a uno o varios textos normativos, entre los que se puede citar especialmente AFNOR Z42013, AFNOR Z42019, MOREQ 1, 2 y 2010, OAIS, ISO 30300, ISO 30301 e ISO 27001.
- 45 **[0012]** En particular, el texto normativo AFNOR Z42013 es aplicable en materia de conservación de informaciones digitales con valor probatorio.
- [0013]** Este texto estipula que cualquier evento relativo a una información digital, para ser oponible, debe estar inscrito en un registro de eventos previsto a tal efecto y almacenado de forma segura.
- 50 **[0014]** Este registro de eventos está asociado a unos medios de trazabilidad que permiten captar automáticamente cada evento relativo a cada información digital almacenada en unos medios de conservación y describir este evento en el registro de eventos.
- 55 **[0015]** La descripción de un evento comprende todo tipo de información complementaria de este evento como, por ejemplo, unas informaciones sobre el autor del evento, sobre su fecha, su manera de ejecutar, sus razones, el número de repetición, etc.
- [0016]** Se conoce igualmente un sistema de gestión de informaciones digitales descrito en el documento US

2012/137367 A1.

**[0017]** No obstante, los sistemas informáticos de gestión segura existentes no son del todo satisfactorios.

5 **[0018]** Más particularmente, estos sistemas no permiten trazar los eventos relativos a las informaciones digitales durante todo el ciclo de vida de estas informaciones.

**[0019]** En efecto, ciertos de estos sistemas permiten únicamente trazar los eventos relativos a las informaciones digitales durante la fase de conservación de estas informaciones digitales.

10

**[0020]** Otros sistemas informáticos de gestión segura aseguran además la trazabilidad de las informaciones digitales durante, por ejemplo, la fase de producción de estas informaciones, pero no permiten tener una vista completa sobre el conjunto de eventos ocurridos durante el ciclo de vida completo de estas informaciones.

15 **[0021]** La presente invención tiene como objeto proponer un sistema informático de gestión segura de informaciones digitales que solucionan los inconvenientes precitados.

**[0022]** A tal efecto, la invención tiene como objeto un sistema informático conforme a la reivindicación 1.

20 **[0023]** Según otros aspectos ventajosos de la invención, el sistema informático de gestión segura comprende una o varias de las características de las reivindicaciones 1 a 7.

**[0024]** Estas características y ventajas de la invención se mostrarán con la lectura de la descripción que aparece a continuación, dada únicamente a título de ejemplo no limitativo y realizada en referencia a los dibujos anexos, en los que:

- la figura 1 es una vista esquemática de un sistema informático de gestión segura de informaciones digitales según la invención, constando el sistema especialmente de un registro de eventos; y

- la figura 2 es una vista esquemática del registro de eventos de la figura 1.

30

**[0025]** Se ha representado en efecto en la figura 1, un sistema informático de gestión segura de informaciones digitales según la invención.

**[0026]** Este sistema está designado por la referencia general 10 en la figura 1.

35

**[0027]** El sistema 10 es utilizable especialmente en el campo del archivo numérico de documentos electrónicos.

**[0028]** Así, según este ejemplo de aplicación, cada información digital comprende un documento electrónico.

40

**[0029]** El sistema 10 comprende unos medios de producción de informaciones digitales, unos medios de conservación de informaciones digitales, unos medios de difusión y de consumo de informaciones digitales y unos medios de trazabilidad de informaciones digitales.

45 **[0030]** Estos medios diferentes están designados respectivamente por las referencias generales 12, 14, 16 y 18 en la figura 1.

**[0031]** Los medios de producción 12 permiten generar unas informaciones digitales de manera conocida en sí en el estado de la técnica.

50

**[0032]** En el campo del archivo numérico, estos medios de producción 12 comprenden, por ejemplo, un calculador apto para recibir unos datos digitales que se van a archivar y formar a partir de estos datos, un archivo que se va a almacenar.

55 **[0033]** Los medios de conservación 14 comprenden, por ejemplo, uno o varios servidores conectados y aptos para almacenar unas informaciones digitales de manera segura.

**[0034]** Estas informaciones son almacenadas, por ejemplo, de manera redundante con un acceso limitado y controlado por unos medios de seguridad previstos a tal efecto.

- 5 **[0035]** Los medios de difusión y de consumo 16 permiten extraer unas informaciones digitales conservadas en los medios de conservación 14, para transmitir estas informaciones a un usuario o para utilizarlas con otros fines predeterminados.
- [0036]** Así, por ejemplo, en el campo del archivo numérico, estos medios 16 forman una interfaz de comunicación con el usuario que permiten consultar especialmente los archivos conservados.
- 10 **[0037]** Se concibe entonces que los medios de producción 12, los medios de conservación 14 y los medios de difusión y de consumo 16 aseguran la gestión de las informaciones digitales durante el ciclo de vida completo de estas informaciones.
- 15 **[0038]** El ciclo de vida de cada información digital se ilustra esquemáticamente por una flecha 20 en la figura 1 y comprende especialmente una fase de producción asegurada por los medios de producción 12, una fase de conservación asegurada por los medios de conservación 14 y una fase de consumo asegurada por los medios de difusión y de consumo 16.
- 20 **[0039]** Además, los medios de producción 12, los medios de conservación 14 y los medios de difusión y de consumo 16 son, por ejemplo, unos medios heterogéneos, situados en unos lugares geográficos distintos e implementados según unas tecnologías diferentes.
- [0040]** Los medios de trazabilidad 18 constan de unos medios de detección de eventos relativos a cada información digital, un registro de estos eventos y un módulo de seguridad del registro.
- 25 **[0041]** Estos componentes diferentes de los medios de trazabilidad 18 están designados respectivamente por las referencias generales 22, 24 y 26 en la figura 1.
- [0042]** Se comprende así por «evento», cualquier acción ejercida por un usuario o por un sistema informático en una información digital.
- 30 **[0043]** Así, por ejemplo, cada evento se escoge en el grupo que consta al menos de:
- creación de una información digital;
  - modificación de una información digital;
  - 35 - supresión de una información digital;
  - duplicación de una información digital;
  - difusión de una información digital; y
  - consulta de una información digital.
- 40 **[0044]** En el ejemplo de la figura 1, los medios de detección 22 se presentan en forma de un módulo de detección 22 independiente de los medios de producción 12, de los medios de conservación 14 y de los medios de difusión y de consumo 16.
- 45 **[0045]** Como variante, los medios de detección 22 se presentan en forma de tres módulos de detección independientes integrados en los medios de producción 12, los medios de conservación 14 y los medios de difusión y de consumo 16. Cada uno de estos módulos de detección es análogo al módulo de detección 22 de la figura 1.
- 50 **[0046]** El módulo de detección 22 es apto para detectar cada evento relativo a cada información digital durante cada una de las fases del ciclo de vida de esta información digital.
- [0047]** En particular, el módulo de detección 22 es apto para detectar cada evento relativo a esta información digital durante la producción de esta por los medios de producción 12, durante la conservación de esta por los medios de conservación 14 y durante la difusión o el consumo de esta por los medios de difusión y de consumo 16.
- 55 **[0048]** El módulo de detección 22 está realizado, por ejemplo, en forma de un programa aplicado independientemente de unos medios de producción 12, unos medios de conservación 14 y unos medios de difusión y de consumo 16 de informaciones digitales.
- [0049]** El módulo de detección 22 es apto, además, para registrar cada evento detectado en el registro de

eventos 24 según un formato de registro común para el conjunto de los eventos.

**[0050]** Como complemento, el módulo de detección 22 es apto para registrar en el registro 24 unos metadatos que acompañan a cada evento.

5

**[0051]** Estos metadatos comprenden, por ejemplo, la fecha del evento, el identificador del autor del evento, el número de repeticiones, etc.

**[0052]** Así, el registro de eventos 24 está dividido entre los medios 12, 14 y 16 y permite registrar el conjunto de eventos ocurridos en estos medios según un formato de registro común.

10

**[0053]** El módulo de seguridad 26 permite proteger el registro de eventos 24 según una tecnología de seguridad conforme, por ejemplo, a un texto normativo tal como AFNOR Z42013.

15

**[0054]** El registro de eventos 24 bajo una forma segura aplicada por el módulo de seguridad 26, está ilustrado de forma esquemática en la figura 2.

**[0055]** Así, en referencia a esta figura, el registro de eventos 24 se presenta en forma de una secuencia de ficheros informáticos designados por las referencias generales 30A a 30N.

20

**[0056]** Cada fichero informático 30A a 30N comprende un encabezado 32A a 34N y un cuerpo 34A a 34N.

**[0057]** El encabezado 32A a 32N de cada fichero informático 30A a 30N siguiente consta de una impresión del fichero informático 30A a 30N anterior en la secuencia.

25

**[0058]** Cada impresión está realizada, por ejemplo, según una técnica de codificación conocida en sí.

**[0059]** El cuerpo 34A a 34N de cada fichero informático 30A a 30N consta de unos registros correspondientes al menos a ciertos eventos detectados por el módulo de detección 22, por ejemplo, según un orden cronológico de estos eventos.

30

**[0060]** Así, en el ejemplo de la figura 2, el encabezado 32B del fichero informático 30B consta de una impresión del fichero informático 30A.

35

**[0061]** Los ficheros 30A a 30N forman así un conjunto continuo lo que permite evitar cualquier modificación ilegítima del registro de eventos 24 como, por ejemplo, una supresión o un añadido de un registro no autorizado.

**[0062]** El funcionamiento del sistema 10 se va a explicar en adelante.

40

**[0063]** Así, durante cada una de las fases de vida de una información digital, el módulo de detección 24 detecta cada evento relativo a esta información digital.

**[0064]** Después, el módulo de detección 22 registra cada evento detectado en el registro 26 de forma segura.

45

**[0065]** Para ello, el módulo de detección 22 transmite el registro correspondiente eventualmente con unos metadatos asociados, al módulo de seguridad 26 que añade un nuevo registro en el último fichero de la secuencia de los ficheros 30A a 30N existentes o crea un nuevo fichero en esta secuencia para este registro.

**[0066]** Por supuesto, otros ejemplos de realización de la invención son igualmente posibles.

50

**[0067]** Se concibe entonces que la presente invención consta de un cierto número de ventajas.

**[0068]** En particular, el sistema según la invención permite trazar cada evento relativo a cada información digital durante cada una de las fases de vida de esta información.

55

**[0069]** La detección y el registro de estos eventos se efectúan de manera centralizada por unos medios de detección independientes.

**[0070]** Esto permite entonces obtener una vista completa sobre el conjunto de los eventos relativos a una

información digital dada.

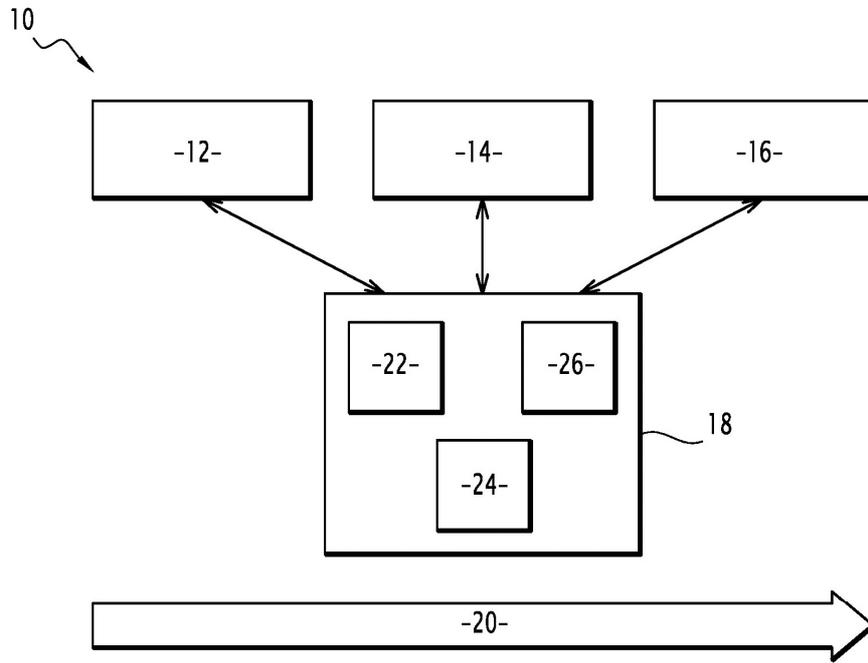
**[0071]** Además, cada evento se registra utilizando un formato único lo que evita la necesidad de tener un tratamiento específico para cada una de las fases de vida de la información digital correspondiente.

5

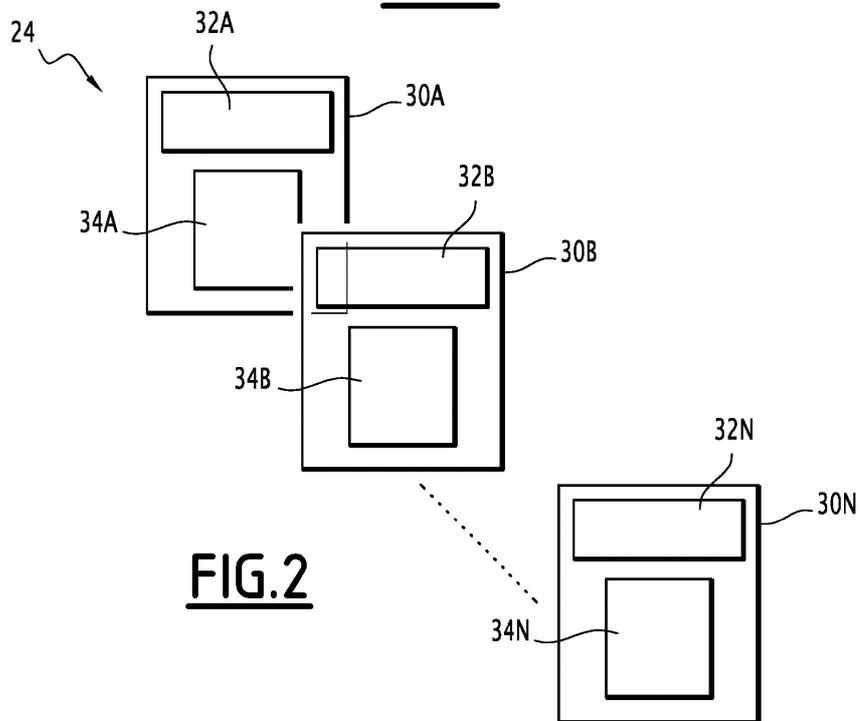
**[0072]** Finalmente, el registro de eventos se almacena de manera centralizada y segura lo que permite satisfacer las exigencias de diferentes textos normativos para asegurar especialmente el valor probatorio de cada información digital.

## REIVINDICACIONES

1. Sistema informático (10) de gestión segura de informaciones digitales que aplican la trazabilidad con valor probatorio de estas informaciones digitales, siendo el sistema especialmente utilizable en el campo del archivo  
5 numérico y que comprende:
- unos medios de producción (12) de informaciones digitales;
  - unos medios de conservación (14) de informaciones digitales;
  - unos medios de difusión y de consumo (16) de informaciones digitales;
- 10 - unos medios de trazabilidad (18) de informaciones digitales que constan de un registro de eventos (24) relativos a unas informaciones digitales y unos medios de detección (22) aptos para detectar cada evento relativo a cada información digital conservada en los medios de conservación (14), para registrar este evento en el registro de eventos (24);
- 15 y en el que
- los medios de detección (22) son aptos para detectar además cada evento relativo a cada información digital durante la producción de esta por los medios de producción (12) y durante la difusión o el consumo de esta por los medios de difusión y de consumo (16), para registrar este evento en el registro de eventos (24) que está dividido entre los  
20 medios de producción (12), los medios de conservación (14) y los medios de difusión y de consumo (16); estando el sistema (10) **caracterizado porque**
- los medios de trazabilidad (18) constan además de un módulo de seguridad (26) que permite proteger el registro de eventos, siendo el módulo de seguridad (26) apto para presentar el registro de eventos (24) en forma de una secuencia de ficheros informáticos (30A,...,30N), comprendiendo cada fichero informático (30A,...,30N) siguiente un  
25 encabezado (32A,...,32N) que consta de una impresión de un fichero informático anterior y un cuerpo (34A,...,34N) que consta de unos registros correspondientes al menos a ciertos eventos detectados por los medios de detección (22).
2. Sistema (10) según la reivindicación 1, **caracterizado porque** los medios de detección (22) son aptos  
30 para registrar cada evento en el registro de eventos (24) según un formato de registro común para el conjunto de los eventos.
3. Sistema (10) según una cualquiera de las reivindicaciones anteriores, **caracterizado porque** cada  
35 evento se escoge en el grupo que consta al menos de:
- creación de una información digital;
  - modificación de una información digital;
  - supresión de una información digital;
  - duplicación de una información digital;
- 40 - difusión de una información digital; y
- consulta de una información digital.
4. Sistema (10) según una cualquiera de las reivindicaciones anteriores, **caracterizado porque** los  
45 medios de detección se presentan en forma de tres módulos de detección (22) independientes integrados en los medios de producción (12), los medios de conservación (14) y los medios de difusión y de consumo (16).
5. Sistema (10) según una cualquiera de las reivindicaciones 1 a 3, **caracterizado porque** los medios de  
50 detección se presentan en forma de un módulo de detección (22) independiente de los medios de producción (12), de los medios de conservación (14) y de los medios de difusión y de consumo (16).
6. Sistema (10) según la reivindicación 4 o 5, **caracterizado porque** el o cada módulo de detección (22) se realiza en forma de un programa.
7. Sistema (10) según cualquiera de las reivindicaciones anteriores, **caracterizado porque** cada  
55 información digital comprende un documento electrónico.



**FIG. 1**



**FIG. 2**