(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 968 093**

(51) Int. Cl.:

G06F 21/64 (2013.01)
H04L 9/32 (2006.01)
H04N 21/266 (2011.01)
H04N 21/835 (2011.01)
H04L 9/00 (2012.01)
H04N 21/2743 (2011.01)
H04N 21/4223 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.06.2022 E 22182372 (7)**

(97) Fecha y número de publicación de la concesión europea: **18.10.2023 EP 4113344**

(54) Título: **Método y sistema de certificación de hechos jurídicos**

(30) Prioridad:

01.07.2021 FR 2107148

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.05.2024

(73) Titular/es:

BP VENTURES (100.0%)
25 Avenue Edouard VII
64200 Biarritz, FR

(72) Inventor/es:

VERHOEK, ROBBERT OTTO;
NOËL, WILFRIED;
LALANNE, JULIEN y
SANTRAILLE, JEAN DOMINIQUE

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y sistema de certificación de hechos jurídicos

La invención hace referencia a un método y un sistema para certificar hechos jurídicos por medio de medios digitales. Entendemos por medios digitales (o "digital media" en inglés) todos los medios (fotografías, vídeos, instantáneas tridimensionales, ficheros de audio, etc.) codificados en formatos legibles por máquinas, es decir, codificados en forma de números. Los medios digitales se pueden crear, visualizar, distribuir, modificar y almacenar en un aparato electrónico digital o transmitirse por Internet en forma de datos representados por una serie de números. Los términos medios digitales también se pueden utilizar como sinónimo.

Entendemos por hecho jurídico cualquier acontecimiento o situación, intencionado o no, que tiene como consecuencia producir efectos jurídicos.

A modo de ejemplo de hechos jurídicos cabe citar los daños causados por una inundación o una catástrofe natural, los daños causados por el desgaste o un accidente (por ejemplo, grietas en muros o fachadas, estado del pavimento, vallas o cercados dañados) o cualquier otro trastorno (abandono o retraso de las obras, defectos, consecuencias de una fuga de agua, contaminación o vertido ilegal de basuras, etc.). Se puede también citar como hecho jurídico los trastornos antes, durante o en el momento de la recepción de las obras, la firma de un contrato, la entrega de bienes o productos, la visualización de una ordenanza municipal o de un aviso de licencia de obras.

La presente invención tiene por objetivo ofrecer un método y un sistema que permita crear pruebas con un alto valor probatorio de un hecho jurídico.

En efecto, en muchas legislaciones, la prueba de un hecho jurídico puede aportarse por cualquier medio. Sin embargo, el valor probatorio varía en función de los medios utilizados.

Por ejemplo, podría ser una simple foto tomada por cualquier usuario por medio de su teléfono, tableta o cámara. Esta prueba tiene poco valor probatorio, similar al de una información, porque la foto puede haber sido retocada y/o el usuario puede haber truncado la escena.

Por el contrario, muchos países disponen de sistemas de recogida de pruebas con un valor probatorio muy elevado.

En Francia, por ejemplo, conocemos el Acta de comprobación elaborado por un agente judicial. Para obtener dicha comprobación, el agente judicial se debe desplazar al lugar para observar personalmente el hecho jurídico. A continuación, hace constar lo que ha observado en un Acta. Estas observaciones son vinculantes mientras no se demuestre lo contrario.

Sin embargo, organizar un informe de este tipo puede llevar mucho tiempo, requiere que el agente judicial se desplace al lugar y conlleva unos costes que pueden ser demasiado elevados en relación con las cuestiones jurídicas en juego.

Ya existen aplicaciones informáticas que tienen por objetivo certificar los medios digitales.

Con este tipo de aplicación, un usuario envía fotografías de un hecho jurídico a un agente judicial para su marcado en el tiempo. Tras recibir las fotografías, el agente judicial emite en unos minutos un Acta automática o casi automática, en la que simplemente estampa una copia de su firma manuscrita.

Un Acta de este tipo tiene muy poco valor probatorio, porque el origen y la sinceridad de las fotografías no están garantizados, ya que pueden haber sido retocadas o manipuladas previamente. Además, el agente judicial o tercero de confianza que certifica las fotografías es siempre el mismo, lo que puede debilitar el valor probatorio del Acta, dependiendo de las legislaciones. Por último, la identidad de la persona que registra las fotografías no es segura, ya que en el Acta se estampa una simple copia de la firma, copia que se puede adquirir fácilmente de Actas en línea ya firmadas. Por tanto, no es posible demostrar que haya sido un agente judicial o un tercero de confianza quien haya levantado el Acta. También existen sistemas de certificación de imágenes digitales, que consisten en estampar un sello de verificación a la imagen. A este respecto podemos citar los documentos US2019/325164, US2014/049653 y US2006115111. Sin embargo, la imagen inicial se podría falsificar antes de la estampación del sello, sin que el sistema pudiera identificar el fraude.

Uno de los objetivos de la presente invención es, por tanto, ofrecer un método y un sistema para certificar hechos jurídicos con un gran valor probatorio, de forma que sea difícil impugnarlos y difícil aportar pruebas en contrario, y que al mismo tiempo sea económico, ecológico, fácil y rápido de aplicar.

La idea que sostiene la invención es ofrecer un método y un dispositivo que creen un vínculo entre un tercero de confianza y el hecho jurídico, sin que el tercero tenga que desplazarse in situ, ni el usuario pueda intervenir o interferir durante este vínculo. En otras palabras, la idea de la invención es simular la presencia del tercero in situ creando un

vínculo entre él y el hecho jurídico, y garantizar que este vínculo no pueda ser corrompido para que el valor probatorio de la certificación sea óptimo y sea difícil, si no imposible, impugnar la materialidad del hecho jurídico.

En otras palabras, la invención ofrece un método y un sistema que permiten a cualquier usuario capturar y enviar de forma segura medios digitales representativos de un hecho jurídico, sin posibilidad de acceder a ellos ni modificarlos, a un tercero de confianza, como por ejemplo, un agente judicial, un experto en un oficio, una persona con competencia para juzgar la conformidad, una solución que utiliza la inteligencia artificial que permite verificar la conformidad, para que este último pueda certificar la recepción, la ausencia de modificación, el fechado en el tiempo y la geolocalización.

En la presente invención, los medios digitales (o "digital media" en inglés) pueden ser una o más fotografías (que son tomas digitales individuales), o vídeos (que son secuencias de instantáneas), tomadas por un aparato de captura equipado con una cámara digital, como por ejemplo, un teléfono inteligente, una tableta digital, un ordenador portátil, un reloj electrónico, etc.

Un medio digital en el contexto de la invención también puede ser una instantánea tridimensional, por ejemplo, consistente en un conjunto de datos de distancia entre el aparato y el objetivo (el hecho jurídico) obtenidos por un sensor de distancia, preferiblemente un escáner LIDAR (por "light detection and ranging" o "laser detection and ranging" en inglés), o bien en español "detección y estimación de la distancia por medio de la luz" o "por láser».

Más concretamente, la invención tiene por objetivo un método de certificación por un tercero de confianza de medios digitales representativos de un hecho jurídico, capturados por un usuario por medio de un aparato de captura de medios digitales, tales como fotografías o vídeos, estando equipado el aparato con una cámara digital, una biblioteca de almacenamiento nativo de medios digitales, una interfaz hombre/máquina y un emisor/receptor que puede transmitir los medios digitales al menos a un servidor remoto por medio de una red de telecomunicaciones. El método se caracteriza porque comprende los siguientes etapas:

a) crear una memoria dedicada en el aparato, diferente de la biblioteca nativa e inaccesible para el usuario, para procesar y/o almacenar los medios digitales a certificar, y prohibir el registro de medios digitales en la biblioteca nativa del aparato de captura;

b) mostrar una orden de activación en la interfaz para iniciar una acción de certificación;

c) cuando la orden de activación ha sido seleccionada por parte del usuario, solicitar la toma de al menos una, preferiblemente al menos dos, ventajosamente al menos tres instantáneas del hecho jurídico por parte del usuario, para crear al menos un medio digital a certificar;

d) generación de un fichero a certificar que incluya dicho al menos un medio digital a certificar, un horario de instantáneas de dicho al menos un medio digital a certificar y coordenadas geográficas del aparato a la hora de la instantánea;

e) si no se puede establecer una conexión a la red de telecomunicaciones, almacenar temporalmente el fichero a certificar en la memoria dedicada inaccesible para el usuario durante una duración predeterminada y, si se puede establecer una conexión a la red de telecomunicaciones, transmitir el fichero a certificar al servidor de almacenamiento remoto por medio de la red de telecomunicaciones;

g) transmitir a un tercero de confianza el fichero a certificar que comprende dicho al menos un medio digital a certificar para su certificación;

h) emitir y registrar en el servidor remoto un acta de certificación si el al menos un medio digital está certificado, o emitir y transmitir al usuario una advertencia de no certificación si el al menos un medio digital no está certificado.

Gracias a la memoria dedicada y a la prohibición de registro de instantáneas en la biblioteca nativa, se crea un vínculo directo entre el objetivo de la cámara del aparato de captura y el servidor remoto al que accede el tercero de confianza, sin que el usuario pueda interferir. Además, el fechado en el tiempo y las coordenadas de geolocalización insertadas automáticamente garantizan la trazabilidad y el seguimiento de las instantáneas y certifican su ubicación. Por último, al exigir que las instantáneas se realicen según distintos valores de aumento, se contextualiza el hecho jurídico y es posible garantizar, comparando las tomas, que no han sido alteradas, lo que refuerza aún más la integridad del método.

De acuerdo con formas de realización particulares:

- la etapa d) puede comprender además la estampación de un marcado único en dicho al menos un medio digital a certificar para crear al menos un medio digital marcado;

- el marcado puede ser esteganográfico;

- el método de certificación también puede comprender, además, entre la etapa e) y la etapa g), una etapa f) de comprobación de la conformidad del marcado único en dicho al menos un medio digital a certificar;

- la etapa g) puede comprender una etapa g1) de transmisión a un tercero de confianza de un mensaje de advertencia de que un fichero a certificar que comprende dicho al menos un medio digital a certificar está presente en el servidor, una etapa g2) de visualización del medio digital a certificar en una interfaz del tercero de confianza cuando el tercero de confianza se conecta al servidor, y una etapa g3) de registro de un acta de certificación en el servidor si el tercero de confianza certifica dicho al menos un medio digital a certificar, o de transmisión de una advertencia de no certificación al usuario si el tercero de confianza no certifica dicho al menos un medio digital a certificar;

- la etapa d) puede comprender además el cifrado del fichero a certificar y/o de los medios digitales a certificar con una clave de cifrado, y la etapa g) comprende la transmisión de una clave de descifrado al tercero de confianza;

- la etapa g) puede comprender una etapa g'1) de transmisión a un tercero de confianza de una clave de descifrado y de un mensaje de advertencia de que un fichero cifrado a certificar que comprende dicho al menos un medio digital a certificar está presente en el servidor, una etapa g'2) de descifrado y visualización del fichero descifrado a certificar en una interfaz del tercero de confianza, cuando el tercero de confianza se conecta al servidor, y una etapa g'3) de registro de un acta de certificación en el servidor si el tercero de confianza certifica dicho al menos un medio digital a certificar, o de transmisión de una advertencia de no certificación al usuario si el tercero de confianza no certifica dicho al menos un medio digital a certificar;

- la etapa g) puede comprender una etapa g"1) de transmisión del fichero cifrado a certificar que comprende dicho al menos un medio digital a certificar, sin clave de descifrado a un primer tercero de confianza custodio, una etapa g"2) de transmisión de la clave de descifrado del fichero cifrado a certificar, sin dicho fichero, a un segundo tercero de confianza custodio, una etapa g"3) de recogida, por un tercero de confianza certificador, del fichero cifrado a certificar y de la clave de descifrado respectivamente del primer y segundo terceros de confianza custodios, una etapa g"4) de descifrado y visualización del fichero descifrado a certificar en una interfaz del tercero de confianza certificador cuando el tercero de confianza se conecta al servidor, y una etapa g"5) de registro de un acta de certificación en el servidor si el tercero de confianza certificador certifica dicho al menos un medio digital a certificar, o de transmisión de una advertencia de no certificación al usuario si el tercero de confianza certificador no certifica dicho al menos un medio digital a certificar;

- el medio digital a certificar puede ser de tipo fotográfico, comprendiendo la etapa c) la toma de al menos dos, ventajosamente al menos tres, instantáneas del hecho jurídico por parte del usuario, desde un mismo ángulo de visión y según diferentes valores de aumento para crear al menos dos, preferiblemente al menos tres, fotografías digitales a certificar;

- el medio digital a certificar puede ser de tipo vídeo, comprendiendo la etapa c) la toma de una multitud de instantáneas del hecho jurídico por parte del usuario según diferentes valores de aumento y posiblemente diferentes ángulos de visión, para crear al menos un vídeo digital a certificar;

- las coordenadas geográficas del aparato registradas en la etapa d) se pueden medir en la hora de cada instantánea y, a continuación, procesarse para obtener una posición geográfica media entre una primera instantánea y una última instantánea, registrándose esta posición geográfica media en el fichero a certificar;

- la etapa g) puede comprender una subetapa preliminar g0) de selección del tercero de confianza entre una lista de terceros de confianza prerregistrados, siendo la selección el resultado de una regla de selección;

- la regla de selección puede comprender la comparación de las coordenadas geográficas incluidas en el fichero a certificar con coordenadas geográficas representativas de cada tercero de confianza prerregistrado, y la selección del tercero de confianza geográficamente más cercano a las coordenadas geográficas incluidas en el fichero a certificar;

- cuando el hecho jurídico se sitúa dentro de un área especificada, la etapa c) puede comprender una solicitud de al menos una instantánea fuera del área especificada del hecho jurídico;

- la etapa c) puede comprender la medición automática de la distancia entre el aparato de captura de medios digitales y el hecho jurídico, y la generación de una señal de advertencia cuando el aparato se encuentra a una distancia predeterminada del hecho jurídico para permitir la toma por parte del usuario de al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico según diferentes valores de aumento;

- la etapa c) puede comprender una solicitud de una primera instantánea con un primer valor de aumento y, a continuación, una solicitud de una segunda instantánea con un segundo valor de aumento, diferente del primero y, a continuación, preferiblemente, una solicitud de una tercera instantánea con un tercer valor de aumento, diferente del primero y del segundo, para permitir la toma de al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico por parte del usuario, según diferentes valores de aumento;

- la etapa c) puede comprender una subetapa preliminar c0) de información por parte del usuario de un tamaño aproximado del hecho jurídico, calculándose los valores de aumento primeros, segundos y posiblemente terceros en función del tamaño aproximado del hecho jurídico;

- la etapa b) puede comprender una subetapa preliminar b0) de información de una duración de la acción de certificación;

- la etapa c) puede comprender una solicitud de anotación por parte del usuario para cada medio digital a certificar;

- la etapa c) puede comprender la captura de datos de distancia entre el aparato de captura y el hecho jurídico, y la etapa g) comprende el envío a una impresora 3D de los datos de distancia y una orden para fabricar una reconstrucción tridimensional del hecho jurídico;

- la etapa e) puede comprender el registro de un horario de recepción del fichero a certificar por el servidor de almacenamiento, y la etapa g) comprende el registro de un horario de conexión del tercero de confianza al servidor de almacenamiento, comprendiendo además el método de certificación, una etapa i) de cálculo de un retardo entre el horario en que el fichero a certificar es recibido por el servidor de almacenamiento y el horario en que el tercero de confianza se conecta al servidor de almacenamiento, de comparación del retardo calculado con un periodo de reasignación predeterminado, y de reasignación del fichero a certificar a otro tercero de confianza; y/o

- la etapa e) puede comprender el registro de un horario de recepción del fichero a certificar por el servidor de almacenamiento, comprendiendo además el método de certificación una etapa j) de cálculo del tiempo transcurrido desde el horario de recepción del fichero a certificar por el servidor de almacenamiento, de comparación del tiempo transcurrido desde el horario en que el fichero a certificar fue recibido por el servidor de almacenamiento con un retardo de respuesta predeterminado, y de emisión de un recordatorio al tercero de confianza cuando el horario de recepción del fichero a certificar por parte del servidor de almacenamiento sea mayor que el retardo de respuesta predeterminado.

La invención también tiene por objetivo un sistema de certificación por un tercero de confianza de medios digitales representativos de un hecho jurídico, que comprende al menos un servidor remoto programado para comunicarse por medio de una red de telecomunicaciones con al menos un aparato de captura de medios digitales de un usuario, estando equipado el aparato de captura de una cámara digital, una biblioteca de almacenamiento nativo de los medios digitales capturados accesible por parte del usuario, una interfaz hombre-máquina, y un emisor/receptor que puede transmitir los medios digitales a dicho servidor remoto, caracterizado por que:

- aparato de captura comprende una memoria dedicada separada de la biblioteca nativa, inaccesible para el usuario, para procesar y/o almacenar los medios digitales a certificar; y por que

- el aparato de captura y el servidor están programados para aplicar el método anterior.

De acuerdo con formas de realización particulares:

- el sistema de certificación en el que:

  - el aparato de captura se puede programar para:

    - reservar un espacio de memoria dedicado inaccesible para el usuario y prohibir el registro de medios digitales en la biblioteca nativa del aparato de captura:

    - mostrar una orden de activación en la interfaz para iniciar una acción de certificación;

    - cuando la orden de activación ha sido seleccionada por el usuario, solicitar la toma de al menos dos, preferiblemente al menos tres, vistas del hecho jurídico por parte del usuario según diferentes valores de aumento para crear al menos un medio digital a certificar;

- generar un fichero a certificar que comprenda dicho al menos un medio digital a certificar, un horario de instantánea de dicho al menos un medio digital a certificar y coordenadas geográficas del aparato a la hora de la instantánea;

- almacenar temporalmente el fichero a certificar si no se puede establecer una conexión a la red de telecomunicaciones, sin que el usuario pueda modificarlos o borrarlos después de haber realizado la instantánea;

- transmitir el fichero a certificar al servidor remoto si se puede establecer una conexión a la red de telecomunicaciones, sin que el usuario pueda modificarlos o borrarlos después de haber realizado la instantánea; y

- el servidor se puede programar para:

  - transmitir el fichero a certificar que comprende dicho al menos un medio digital a certificar a un tercero de confianza para su certificación;

  - emitir y registrar un acta de certificación (114) si el medio digital está certificado, o emitir y transmitir al usuario una advertencia de no certificación si el medio digital no está certificado;

- el aparato de captura también se puede programar para estampar un marcado único en dicho al menos un medio digital a certificar para crear al menos un medio digital marcado;

- el aparato de captura puede comprender además un sensor de distancia, estando programado el aparato para medir automáticamente una distancia entre el aparato de captura de medios digitales y el hecho jurídico, y para generar una señal de advertencia cuando el aparato se sitúe a una distancia predeterminada del hecho jurídico para permitir la toma por parte del usuario de al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico según diferentes valores de aumento;

- el sensor de distancia puede estar asociado a un sistema de barrido angular programado para realizar un barrido de una zona definida que comprende el hecho jurídico y obtener una o más instantáneas constituidas por datos de distancia, estando programado el aparato de captura para producir una cartografía tridimensional de la superficie de dicha zona a partir de los datos de distancia obtenidos, y generar un fichero a certificar que comprenda dicha cartografía como medio digital a certificar, un horario de obtención de la cartografía, y unas coordenadas geográficas del aparato en el horario de la cartografía;

- el servidor remoto también se puede programar para transmitir al aparato de captura una clave para el marcado de los medios digitales a certificar;

- el servidor remoto también se puede programar para comprobar la conformidad del marcado en cada medio digital a certificar recibido del aparato de captura;

- el servidor remoto también se puede programar para transmitir al aparato de captura una clave de cifrado para el fichero a certificar y/o los medios digitales a certificar y para transmitir a un tercero de confianza una clave de descifrado;

- el servidor remoto también se puede programar para elegir a un tercero de confianza en función de las coordenadas geográficas incluidas en el fichero a certificar; y/o

- el servidor remoto también se puede programar para transmitir el fichero cifrado a certificar, sin clave de descifrado, a un primer tercero de confianza custodio, para transmitir la clave de descifrado del fichero cifrado a certificar, sin dicho fichero, a un segundo tercero de confianza custodio, y para recoger, a solicitud de un tercero de confianza certificador, el fichero cifrado a certificar y la clave de descifrado del primero y segundo terceros de confianza custodios respectivamente.

Otras características de la invención se expondrán en la descripción detallada que figura a continuación hecha con referencia a las figuras adjuntas, que se dan a título de ejemplo y que muestran, respectivamente:

[Fig. 1] es una vista esquemática de un sistema de certificación de acuerdo con la invención; y

[Fig. 2] es un diagrama funcional del método de certificación de acuerdo con la invención.

La Figura 1 ilustra un sistema de certificación 100 para la implementación del método de certificación de acuerdo con la invención.

El sistema 100 comprende al menos un servidor remoto 101 programado para comunicarse por medio de una red de telecomunicaciones 102 con al menos un aparato de captura de medios digitales 103 de un usuario U.

El aparato de captura 103 está equipado con una cámara digital (no ilustrada) que permite la captura de instantáneas bien en forma de fotografías (instantáneas individuales) o bien en forma de vídeo (secuencia de instantáneas).

En una forma de realización ventajosa descrita más adelante, el aparato de captura 103 se puede equipar con un sensor de distancia que permita la captura de instantáneas tridimensionales que comprendan datos sobre la distancia entre el aparato y el objetivo, es decir, en la utilización a la que hace referencia la presente invención, de un hecho jurídico.

Ventajosamente, el aparato de captura 103 es un teléfono inteligente, una tableta o un ordenador portátil comercial, en el que se ha instalado una aplicación informática que permite la implementación del método de acuerdo con la invención.

Este tipo de aparato 103 comprende una interfaz hombre-máquina 104 (generalmente una pantalla táctil o un conjunto de pantalla/teclado/touchpad o ratón) y un emisor-receptor que se puede comunicar con una red de comunicación telefónica y/o de Internet (generalmente un emisor-receptor wifi, LoRa, GSM, 3G, 4G, 5G, etc.). De acuerdo con la invención, la aplicación informática de implementación del método permite transmitir medios digitales al servidor remoto 101 por medio de la red de comunicación 102.

El sistema operativo de este tipo de aparato proporciona de forma nativa, es decir por defecto y sin necesidad de que el usuario lo instale, una biblioteca de almacenamiento nativo de los medios digitales capturados por la cámara y accesible por parte del usuario. De este modo, se pueden consultar las fotografías que se han tomado, compartirlas, modificarlas y/o dar acceso a otras aplicaciones a esta biblioteca para la edición de imágenes, por ejemplo.

En otras palabras, el aparato se programa de forma nativa para registrar todas las instantáneas capturadas por la cámara en esta biblioteca accesible al usuario.

De acuerdo con la invención, el aparato de captura 103 se programa para reservar un espacio de memoria dedicado, diferente de la biblioteca nativa e inaccesible para el usuario, y para prohibir el registro de medios digitales en la biblioteca nativa del aparato de captura.

Por "inaccesible para el usuario" se entiende un espacio de memoria que el usuario no puede consultar, bien porque no tiene acceso al mismo, bien porque no dispone de los derechos de acceso, bien porque no dispone de los códigos de acceso, bien porque no puede identificar la memoria o la parte de memoria en cuestión. En una forma de realización preferida, el espacio de memoria inaccesible para el usuario es un espacio de almacenamiento cifrado para el que el usuario no posee la clave de cifrado, de forma que el usuario no puede consultar ni modificar los datos presentes en este espacio de memoria.

Este espacio de memoria dedicado comprende al menos un primer espacio situado en la memoria de acceso aleatorio del aparato (es decir, volátil) utilizado para llevar a cabo el tratamiento de los medios digitales (marcado y/o cifrado), el fechado en el tiempo, la geolocalización, etc. (véase la descripción de la etapa d) de la Figura 2), y que se borra una vez procesados los medios digitales. Este primer espacio es inaccesible para el usuario, que no puede conocer su dirección en la memoria de acceso aleatorio.

El espacio de memoria dedicado comprende ventajosamente un segundo espacio situado en una memoria de sólo lectura (es decir, no volátil), que es por supuesto diferente de la biblioteca nativa. Este segundo espacio comprende un fichero cifrado al que sólo tiene derechos de acceso la aplicación. Este segundo espacio se utiliza para almacenar temporalmente los medios digitales procesados en el primer espacio de memoria de acceso aleatorio y que no se han podido transmitir a un servidor remoto, por ejemplo, porque el aparato está en modo "fuera de línea".

En otras palabras, este espacio de memoria dedicado se utiliza, en esencia, por la aplicación para procesar las instantáneas (primer espacio en memoria de acceso aleatorio), pero también se puede utilizar para almacenar temporalmente las instantáneas procesadas en caso de que no se pueda establecer una conexión con la red de telecomunicaciones (segundo espacio en memoria de sólo lectura). Lo importante es que, incluso en el caso de almacenamiento temporal, el usuario no pueda acceder a él.

En una forma de realización particular, el segundo espacio en memoria de sólo lectura, o un tercer espacio en memoria de sólo lectura diferente del segundo, es/son utilizado/s por parte de la aplicación para almacenar herramientas de procesamiento (clave de marcado, clave de cifrado).

El aparato de captura 103 también se programa para mostrar una orden de activación en la interfaz para iniciar una acción de certificación.

Ventajosamente, esta orden incluye una solicitud de información sobre los identificadores del usuario con el fin de asociarlo a su espacio personal en el servidor remoto. Este espacio personal puede ser consultado a distancia por parte del usuario e incluye las Actas de los medios digitales ya certificadas por un tercero de confianza.

Cuando la orden de activación ha sido seleccionada por parte del usuario, el aparato de captura 103 se programa para solicitar la toma de al menos una, preferiblemente al menos dos, ventajosamente al menos tres instantáneas del hecho jurídico por parte del usuario, según diferentes valores de aumento.

En la Figura 1 se ilustra un ejemplo de forma de realización en la que la pantalla 104 del teléfono inteligente 103 muestra tres iconos 104a, 104b, 104c que representan tres valores de aumento diferentes.

Al pulsar el icono 104a, el usuario activa la cámara y toma una foto de plano general 105a, por ejemplo. En la Figura 1, esta foto 105a representa una casa M vista en su totalidad y cuya fachada presenta una grieta F.

Al pulsar el icono 104b, el usuario activa la cámara y toma una foto de plano medio 105b, por ejemplo. En la Figura 1, esta foto 105b representa una parte de la fachada de la casa M que tiene una grieta F.

Por último, pulsando el icono 104c, el usuario activa la cámara y toma una foto de primer plano 105c, por ejemplo. En la Figura 1, esta foto 105c representa la grieta F y permite distinguir los detalles.

De este modo, el aparato de captura puede crear al menos un medio digital a certificar y, en el caso del ejemplo descrito, tres medios digitales (tres fotografías 105a, 105b, 105c) a certificar.

En una forma de realización alternativa particular, el orden de las instantáneas en función del valor de aumento puede ser impuesto por el sistema al usuario.

Preferiblemente, el aparato de captura se programa para mostrar un campo de comentarios frente a cada elemento de medio digital a certificar, de forma que el usuario pueda realizar anotaciones en el medio. Esta forma de realización se reserva preferiblemente para el modo en línea. De este modo, ventajosamente, en el modo fuera de línea, el aparato de captura se programa para no mostrar un campo de comentarios para evitar cualquier riesgo de que los comentarios se modifiquen antes de que se envíen las instantáneas cuando el aparato vuelva a estar en línea.

Preferiblemente, el aparato de captura se programa para guiar al usuario en la captura de instantáneas con diferentes valores de aumento.

Por ejemplo, la aplicación muestra una solicitud de una primera instantánea con un primer valor de aumento y, a continuación, una vez capturada la primera vista, una solicitud de una segunda instantánea con un segundo valor de aumento, distinto del primero. A continuación, preferiblemente una vez capturada la segunda vista, la aplicación muestra una solicitud de una tercera instantánea a un tercer valor de aumento, distinto del primero y del segundo, y así sucesivamente, para permitir que el usuario capture al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico, según diferentes valores de aumento.

Los diferentes valores de aumento se pueden obtener de dos maneras distintas: o bien el usuario mantiene el mismo valor de zoom del aparato de captura y se acerca al hecho jurídico para capturar las diferentes instantáneas, o bien el usuario permanece a la misma distancia del hecho jurídico y cambia el valor del zoom.

Cuando el medio digital a certificar es de tipo fotográfico, el aparato de captura se programa preferiblemente para solicitar la captura de instantáneas de diferentes valores de aumento manteniendo el mismo ángulo de visión, lo que permite limitar los riesgos de manipulación de la imagen y, en última instancia, permitirá al tercero de confianza certificar que las fotografías están efectivamente vinculadas entre sí por un hecho jurídico común.

Esta precaución de mantener el mismo ángulo de visión no es necesaria en el caso del vídeo, ya que el tercero de confianza podrá identificar visualmente la trayectoria del usuario durante la captura del vídeo. De este modo, cuando el medio digital a certificar es de tipo vídeo, la toma del vídeo (que se compone de una serie de instantáneas) se puede hacer según diferentes valores de aumento y diferentes ángulos de visión para crear el vídeo digital a certificar.

En una forma de realización alternativa preferida, la orientación del usuario recibe en materia de la diferencia entre los distintos valores de aumento es más importante, lo que permite garantizar la calidad de las instantáneas, especialmente en el caso de las fotografías.

Para este fin, el aparato de captura incluye también un sensor de distancia que puede estar ya integrado en el aparato o añadido mediante la agregación de un objetivo desmontable equipado con un sensor de distancia integrado. Un sensor de este tipo permite respetar las distancias entre instantáneas en función del tamaño del hecho jurídico a

identificar. Preferiblemente, en este caso, el aparato de captura se programa para almacenar, para cada instantánea, la información de distancia entre el aparato de captura y el hecho jurídico, con el fin de permitir el análisis posterior del aumento y la distancia por parte del tercero de confianza, y juzgar la coherencia entre las diferentes instantáneas.

Se puede tratar por ejemplo, de un telémetro ultrasónico, un telémetro de infrarrojos, un telémetro láser o un escáner LIDAR.

Preferiblemente, el aparato de captura 103 se programa para mostrar en la interfaz una solicitud de información por parte del usuario de un tamaño aproximado del hecho jurídico, lo que permite a el aparato de captura calcular los primeros, segundos y posiblemente terceros (o incluso superiores) valores de aumento en función del tamaño aproximado del hecho jurídico.

Por ejemplo, el aparato de captura se puede programar para solicitar la captura de instantáneas respectivamente a:

- 10 metros (plano general), 5 metros (plano medio) y 1 metro (primer plano) para un objetivo (el hecho jurídico) de menos de cincuenta centímetros de longitud;
- 20 metros (plano general), 10 metros (plano medio) y 3 metros (primer plano) para un objetivo (el hecho jurídico) comprendido entre cincuenta centímetros y dos metros de longitud;
- 30 metros (plano general), 15 metros (plano medio) y 5 metros (primer plano) para un objetivo (el hecho jurídico) de más de dos metros de longitud.

Estos valores se dan a título de ejemplo no restrictivo y pueden ser ajustados por el usuario o gestor del sistema de acuerdo con la invención en función del tipo de hecho jurídico a capturar.

De este modo, de acuerdo con esta forma de realización alternativa de la invención, el aparato de captura 103 se programa para medir de forma automática una distancia entre el aparato de captura de medios digitales y su objetivo (el hecho jurídico), y para producir una señal de advertencia cuando el aparato se encuentre a una distancia determinada del hecho jurídico calculada por el aparato. De este modo, el aparato permite la toma de al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico por parte del usuario, según diferentes valores de aumento, lo que garantiza que el tercero de confianza pueda establecer el vínculo entre las instantáneas y contextualizar el hecho jurídico y le permite certificar la autenticidad de las instantáneas.

La señal de advertencia puede ser audible o visual en el aparato de captura.

Dependiendo del modo de captura elegido, o bien el usuario mantiene el mismo valor de zoom de la cámara y se acerca al objetivo, en cuyo caso el cálculo de la distancia entre el aparato y el objetivo es útil para saber cuándo detenerse a capturar la siguiente instantánea, o bien permanece a la misma distancia del objetivo, y el usuario cambia el valor del zoom. En este caso, el aparato indicará los valores de zoom adecuados para las diferentes instantáneas, preferiblemente en función del tamaño aproximado del hecho jurídico que se haya introducido previamente.

Ventajosamente, el sensor de distancia se puede utilizar para realizar instantáneas tridimensionales por sí mismo, en lugar de limitarse a indicar valores de aumento al usuario.

Para este fin, el sensor de distancia se asocia a un sistema de barrido angular programado para efectuar un barrido de una zona definida que comprende el hecho jurídico y obtener una o más instantáneas constituidas por datos de distancia. Ventajosamente, un sensor de este tipo es un escáner LIDAR.

Equipada de este modo, el aparato de captura está programado para producir una cartografía tridimensional de la superficie de dicha zona a partir de los datos de distancia obtenidos, siendo dicha cartografía el medio digital a certificar.

Una vez capturadas las instantáneas, el aparato de captura 103 de acuerdo con la invención también está programado para generar un fichero a certificar 106 que comprende dicho al menos un medio digital a certificar (en la Figura 1: las tres fotografías, pero también puede ser un vídeo o una cartografía tridimensional), una marca de tiempo 107 de la instantánea de dicho o cada medio digital a certificar y las coordenadas geográficas 108 del aparato en la marca de tiempo de la instantánea.

Para este fin, la aplicación se programa para acceder al reloj interno del aparato digital y registrar la marca de tiempo (hora y la fecha) de cada instantánea. Además, accede al sensor GPS (u otro) del aparato de captura y registra las coordenadas de geolocalización del aparato de captura en la marca de tiempo de la instantánea. Como alternativa o en combinación, la aplicación de acuerdo con la invención se programa para recuperar los datos de geolocalización del aparato desde una aplicación dedicada presente en el aparato, por ejemplo, destinada a mejorar la precisión de los datos de geolocalización del GPS (u otro) sensor.

De este modo, el fichero a certificar 106 incluye las instantáneas, pero también los datos de marca de tiempo (fecha y hora) y las coordenadas geográficas relativas a cada instantánea (o al conjunto de instantáneas en el caso de un vídeo; en este caso, es posible registrar únicamente la hora de inicio y la hora de fin o la duración del vídeo).

También se puede captar y registrar otra información, como por ejemplo, la altimetría, la temperatura, etc.

En una forma de realización ventajosa, las coordenadas geográficas (coordenadas GPS) del aparato almacenadas en el fichero a certificar 106, son el resultado de un cálculo (por ejemplo, una media) realizado sobre las coordenadas geográficas medidas a la hora de cada instantánea.

Un cálculo de este tipo permite utilizar la función de actualización el sensor de datos de geolocalización (GPS, Galileo, etc.) y activar una nueva evaluación de la precisión de los datos de geolocalización, lo que permite a la aplicación conservar o no los datos de geolocalización de cada foto de acuerdo con los criterios de nivel de precisión predefinidos en la aplicación. Esta actualización tiene lugar a medida que se toman las instantáneas, con el fin de conservar las coordenadas de geolocalización más fiables.

En cualquier caso, estas coordenadas geográficas se recuperan de forma automática y se asignan a los medios a certificar sin que el usuario pueda modificarlas.

Preferiblemente, el método de certificación sólo puede comenzar si el sensor de datos de geolocalización (GPS u otro) del aparato de captura está activo.

En una forma de realización particular, cuando el hecho jurídico a demostrar se encuentra dentro de una zona específica, por ejemplo, dentro de un edificio, el aparato de captura se programa para solicitar que al menos una instantánea se realice fuera del zona específica del hecho jurídico. Esta opción permite contextualizar las instantáneas.

En una forma de realización preferida de la invención, el aparato de captura también se programa para estampar un marcado único 109 en el o los medios digitales a certificar para crear al menos un medio digital marcado.

Ventajosamente, se trata de un marcado esteganográfico modificado por una frecuencia definida por el sistema.

En el caso de las fotografías, se puede marcar cada una de ellas.

A efectos de marcado, el servidor remoto 101 se programa para transmitir al aparato de captura una clave de marcado 110 para los medios digitales a certificar, por ejemplo, cuando la aplicación informática se instala en el aparato de captura o después de que el usuario se conecte, es decir, después de ser identificado por el sistema. Alternativamente, este marcado es creado por el servidor y enviado a la aplicación. El primer marcado es el del día en que se instala la aplicación. A continuación, el servidor envía un nuevo marcado cada día. Si el aparato está desconectado, se asignará el marcado con la fecha de la última actualización. Lo importante es poder asegurar el medio digital desde el momento de su captura, hasta que el tercero de confianza lo certifique.

De este modo, el servidor remoto 101 y/o el tercero de confianza 120 efectúa(n) una comprobación de conformidad del marcado único en el o los medios digitales marcados para garantizar que los medios digitales a certificar han sido efectivamente capturados de acuerdo con el método de acuerdo con la invención.

Como alternativa o en combinación, el aparato de captura también se programa para efectuar una cifrado 111 del fichero a certificar 106 y/o de cada medio a certificar con una clave de cifrado 112, tan pronto como se capturen las instantáneas.

Para el cifrado, el servidor remoto 101 se programa para transmitir al aparato de captura una clave de cifrado 112 para los medios digitales a certificar, preferiblemente cuando se instala la aplicación informática en el aparato de captura o cuando se crea cada carpeta. Este número de cifrado constituye la raíz de cada medio para efectuar el cifrado 111.

Este cifrado es automático e independiente del usuario, de forma que éste no puede abrir los medios a certificar, aunque consiguiera forzar el acceso a la memoria dedicada del aparato (segundo espacio en memoria de sólo lectura).

Como alternativa o en combinación, el aparato de captura también se programa para asignar un identificador único al o a cada medio digital.

Con el fin de asignar este identificador, el servidor remoto 101 se programa para transmitir al aparato de captura un número identificador único para cada medio digital a certificar después de la conexión del usuario, es decir, después de que haya sido identificado por el sistema y tan pronto como se haya capturado un medio digital. Alternativamente, si el aparato de captura está fuera de línea cuando se capturan el o los medios digitales, el servidor remoto 101 se programa para asignar un identificador único al o a cada medio digital tan pronto como el fichero a certificar 106 se reciba en el servidor cuando el aparato de captura vuelva a estar en línea.

En otras palabras, el servidor remoto 101 asigna inmediatamente el número único a cada medio digital cuando el aparato de captura se conecta al servidor remoto 101, o en un momento posterior cuando recibe el fichero a certificar 106 cuando el aparato de captura vuelve a estar en línea. Este número único garantiza la trazabilidad de los medios digitales.

Para que el tercero de confianza pueda ver los medios a certificar, el servidor remoto 101 se programa para enviar al tercero de confianza 120 una clave de descifrado 113 por correo electrónico o cualquier otro medio electrónico (sms, código OR, portal de gestión, etc.) cuando el tercero de confianza desee ver por primera vez los medios a certificar. Esta clave de descifrado no se transmite nunca al usuario, que no puede por tanto modificar los medios una vez cifrados, es decir, en el momento de las instantáneas son capturadas.

Preferiblemente, el usuario no puede acceder a los ficheros que ha enviado para su certificación en su espacio personal hasta que el tercero de confianza haya examinado dichos ficheros. Esto aumenta la seguridad para evitar cualquier modificación posterior de las instantáneas entre el momento en que se realizan y el momento en que son examinadas por el tercero de confianza, lo que mejora aún más el valor probatorio del sistema de acuerdo con la invención y de la certificación por parte del tercero de confianza.

De este modo, una vez que el aparato de captura 103 ha permitido la captura de las instantáneas, les ha puesto la marca de tiempo, las ha geolocalizado, las ha marcado y posiblemente cifrado, y ha creado el correspondiente fichero a certificar 106 (en el primer espacio de memoria de acceso aleatorio), se programa para transmitir el fichero a certificar 106 directamente al servidor remoto 101, si se puede establecer una conexión a la red de telecomunicaciones (modo en línea), y sin que el usuario pueda modificarlas después de haber realizado las instantáneas.

Si no se puede establecer una conexión con la red de telecomunicaciones (modo fuera de línea), el aparato de captura 103 se programa para almacenar temporalmente los medios digitales a certificar (o el fichero a certificar 106) en la memoria dedicada creada de antemano (segundo espacio en la memoria de sólo lectura), sin que el usuario pueda modificarlas después de haber realizado las instantáneas.

Tan pronto como se restablezca la conexión a la red, el aparato de captura 103 se programa para transmitir el fichero a certificar 106 al servidor remoto 101 y para borrar este fichero y los medios digitales del espacio de memoria dedicado (el segundo espacio en la memoria de sólo lectura).

Ventajosamente, el aparato de captura 103 se programa para borrar el fichero a certificar 106 de esta memoria dedicada tras una duración predeterminada (por ejemplo, 12h00) si no ha sido posible transmitir el fichero al servidor remoto, por ejemplo, en el caso de una desconexión prolongada de la red de comunicación 102. Esta forma de realización alternativa permite garantizar que la duración entre las instantáneas y su transmisión no supere un periodo de seguridad más allá del cual un pirateo del sistema podría permitir la manipulación de los medios. También garantiza que la etapa de certificación por parte del tercero de confianza no se aleje demasiado en el tiempo de la captura de las instantáneas, lo que podría debilitar el valor probatorio de la certificación.

Una vez que los medios a certificar han sido recibidos por el servidor remoto en forma de un fichero a certificar 106, el servidor remoto 101 se programa para transmitir a un tercero de confianza el fichero a certificar 106 que comprende dicho al menos un medio digital a certificar 105a-105b-105C y los datos de marca de tiempo 107a-107b-107C y geolocalización 108a-108b-108C, así como, ventajosamente, datos de altimetría, ángulo de visión y/o elevación (ángulo de alabeo, cabeceo y/o guiñada medidos y transmitidos por un giroscopio) del aparato de captura.

En combinación, el aparato de captura de medios puede capturar o recuperar otros tipos de datos y transmitirlos al servidor remoto, como por ejemplo, la temperatura, la hidrometría, la presión atmosférica, la radiactividad, el índice de CO2 o incluso datos del viento (fuerza y dirección). En este caso, el aparato de captura se conecta ventajosamente a un sensor adecuado, como por ejemplo, un higrómetro, un anemómetro, un termómetro, etc.

Si el fichero a certificar 106 está cifrado, el servidor remoto 101 también transmite una clave de descifrado 113 al tercero de confianza 120 para que pueda descifrar el fichero y visualizar los medios a certificar.

Más concretamente, en una primera forma de realización, el servidor remoto 101 se programa para transmitir al tercero de confianza 120 un mensaje de advertencia de que un fichero a certificar 106 que comprende dicho al menos un medio digital a certificar está presente en el servidor y a la espera de certificación.

Una vez que el tercero de confianza se ha conectado al sistema utilizando un identificador/contraseña, el servidor remoto 101 transmite el fichero a certificar 106. Esto se puede hacer descargando el fichero en el ordenador local del tercero de confianza para su posterior consulta y certificación. Alternativamente, esta transmisión se puede realizar mostrando el o los medios digitales a certificar directamente en una interfaz del tercero de confianza.

Si el tercero de confianza certifica los medios, genera un acta de certificación 114 firmada electrónicamente y la registra en el servidor remoto. Este acta de certificación 114 se pone entonces a disposición del usuario en su espacio personal, donde la puede consultar, descargar o compartir con un tercero.

La firma electrónica no es una simple copia digital, sino que se genera mediante un certificado de firma electrónica obtenido de una autoridad de referencia.

El tercero de confianza puede certificar el o los medios digitales contenidos en el fichero a certificar 106 al menos comprobando que dichos soportes han sido efectivamente capturados con el sistema de acuerdo con la invención, lo que le permite garantizar que no han sido almacenados en la biblioteca nativa del aparato de captura 103, y por tanto que no han podido ser modificados por parte del usuario. Ventajosamente, también puede comprobar además que el marcado y/o cifrado de los medios se ajusta a la clave de marcado y/o cifrado. Gracias a estos elementos, se tiene la certeza de que los medios han sido efectivamente capturados con el sistema de acuerdo con la invención y que no han sido modificados desde su captura. También puede certificar el número de medios recibidos. También puede certificar la marca de tiempo y la geolocalización asociadas a cada medio, ya que esta información ha sido añadida de forma automática por el sistema justo después de capturar los medios y antes de enviarlos (directamente en modo "en línea" o tras un almacenamiento temporal, preferiblemente cifrado en una memoria inaccesible para el usuario en modo "fuera de línea") al servidor remoto 101 para su almacenamiento.

En una forma de realización preferida, la certificación comprende una comprobación, por parte del tercero de confianza, de la conformidad de los medios con determinados criterios cualitativos, como por ejemplo, la nitidez de las fotografías, la visibilidad y/o comprensibilidad del hecho jurídico ilustrado por los medios, su conformidad con la ley, etc.

Como alternativa o en combinación, la certificación comprende una comprobación por parte del tercero de confianza de que las instantáneas cumplen un protocolo predefinido, como por ejemplo, el número mínimo de instantáneas requerido, su secuenciación, los diferentes ángulos de visión, etc.

Si el tercero de confianza no certifica al menos uno de los medios a certificar, como por ejemplo, una o dos fotografías de un grupo de tres fotografías, o incluso las tres fotografías del mismo grupo, por ejemplo, porque las instantáneas están borrosas o los valores de aumento no cumplen, genera una notificación de no certificación de esta o estas fotografías, que se registra en el servidor remoto 101.

A continuación, éste último se programa para enviar al usuario una advertencia de no certificación que puede verse en su espacio personal.

En una forma de realización alternativa, el servidor remoto 101 se programa para transmitir el fichero cifrado a certificar 106 que comprende dicho al menos un medio digital a certificar, sin clave de descifrado a un primer tercero de confianza custodio, para que almacene el fichero cifrado. Este primer tercero de confianza puede elaborar ventajosamente un Acta de recepción con el número de ficheros cifrados y eventualmente el número de medios digitales por fichero cifrado recibido, pero como no puede abrirlos, no los puede examinar y certificar su pertinencia, ni modificarlos inadvertidamente.

En paralelo, el servidor remoto 101 se programa para transmitir la clave de descifrado del fichero cifrado a certificar 106, sin dicho fichero, a un segundo tercero de confianza custodio para que almacene la clave de descifrado. Este segundo tercero de confianza puede elaborar ventajosamente un Acta de recepción de la clave de descifrado.

Cuando el usuario necesita que se certifiquen los medios, el servidor remoto, a solicitud del usuario, transmite una instrucción de recogida a un tercero de confianza certificador, ventajosamente distinto del primero y segundo terceros de confianza custodios, para que recoja el fichero cifrado a certificar 106 y la clave de descifrado del primero y segundo terceros de confianza custodios, respectivamente.

Una vez conectado al servidor remoto 101, el tercero de confianza certificador descifra el fichero cifrado a certificar 106 utilizando la clave de descifrado, y lo muestra en una interfaz para su certificación.

Si el tercero de confianza certificador certifica los medios, genera un acta de certificación 114 firmada electrónicamente y lo registra en el servidor remoto. Este acta de certificación 114 se pone entonces a disposición del usuario en su espacio personal, donde la puede consultar, descargar o compartir con un tercero.

Si el tercero de confianza certificador no certifica los medios, por ejemplo, porque las instantáneas son borrosas o los valores de aumento no cumplen, genera una notificación de no certificación para todos o uno o más medios que se registran en el servidor remoto 101.

A continuación, éste último se programa para que envíe al usuario una advertencia si no se ha certificado la totalidad o una parte de los medios.

Preferiblemente, la etapa de transmisión del fichero a certificar 106 a un tercero de confianza comprende una etapa preliminar de selección del tercero de confianza entre una lista de terceros de confianza prerregistrados, resultando la selección de una regla de selección.

En particular, en una forma de realización preferida, el servidor remoto se programa para elegir a un tercero de confianza en función de las coordenadas geográficas incluidas en el fichero a certificar 106.

De este modo, la regla de selección comprende la comparación de las coordenadas geográficas incluidas en el fichero a certificar 106 con las coordenadas geográficas representativas de cada tercero de confianza prerregistrado.

El servidor remoto puede entonces elegir el tercero de confianza geográficamente más cercano a las coordenadas geográficas incluidas en el fichero a certificar 106. Alternativamente, el tercero de confianza se puede elegir al azar o de acuerdo con una regla de preferencia (por ejemplo, el número de certificaciones ya realizadas) entre varios terceros de confianza cuyas coordenadas geográficas representativas se encuentren dentro de una zona geográfica predeterminada alrededor de las coordenadas geográficas incluidas en el fichero a certificar 106. Por ejemplo, en Francia, los agentes judiciales son legalmente competentes en una zona geográfica predeterminada. El servidor remoto puede entonces elegir un tercero de confianza entre varios que sean competentes en la zona geográfica alrededor de las coordenadas geográficas incluidas en el fichero a certificar 106.

El sistema de acuerdo con la invención también permite garantizar el seguimiento de las distintas etapas con el fin de garantizar que la duración entre la creación de los medios a certificar y la certificación no sea demasiado largo, reforzando de este modo el valor probatorio de los medios y del acta.

Preferiblemente, la etapa de transmisión del fichero a certificar 106 al servidor remoto 101 comprende el registro de una hora de recepción del fichero a certificar 106 por parte del servidor remoto 101. Este último también se programa para calcular el tiempo transcurrido desde esta hora de recepción del fichero a certificar, y para comparar el tiempo transcurrido desde la hora de recepción del fichero a certificar y un retardo de respuesta predeterminado, por ejemplo, 48 horas, teniendo en cuenta eventualmente los días laborables.

Cuando la hora de recepción del fichero a certificar 106 por parte del servidor de almacenamiento sea mayor que el retardo de respuesta predeterminado, el servidor de almacenamiento se programa para enviar un recordatorio al tercero de confianza con el fin de que proceda a certificar el fichero.

Preferiblemente, el servidor remoto también se programa para comparar el tiempo transcurrido desde la hora de recepción del fichero a certificar (106) y un periodo de reasignación a otro tercero de confianza cumpliendo una regla de asignación (territorialidad, proximidad del hecho jurídico, disponibilidad, etc.). Además, el servidor remoto también se puede programar para emitir una advertencia al usuario cuando el retardo calculado sea mayor que el periodo de reasignación predeterminado. De este modo, se advierte al usuario de que aún no ha sido posible certificar los medios.

En una forma de realización particular, cuando el medio a certificar consiste en un conjunto de datos de distancia que representan una cartografía tridimensional del hecho jurídico, la etapa de transmisión del fichero a certificar 106 comprende el envío de los datos de distancia a una impresora 3D y una orden para producir una reconstrucción tridimensional del hecho jurídico.

La Figura 2 es un diagrama que ilustra el método de certificación de acuerdo con la invención aplicado por el sistema de certificación descrito anteriormente.

En la etapa a), el método consiste en crear una memoria dedicada en el aparato, inaccesible para el usuario, para procesar y/o almacenar los medios digitales a certificar, y prohibir el registro de medios digitales en la biblioteca nativa del aparato de captura.

En la etapa b), el método consiste en mostrar una orden de activación en la interfaz para iniciar una acción de certificación. La etapa b) puede comprender una subetapa preliminar b0) de información de una duración para la acción de certificación. Esta duración define el tiempo durante el cual los medios a certificar pueden ser capturados.

Por ejemplo, el usuario puede tomar fotografías durante un periodo de cinco días en la misma carpeta. Para ello, el primer día selecciona la orden "certificar durante 5 días". Los medios digitales tomados cada día ya no podrán modificarse ni comentarse al día siguiente de su instantánea, con el fin de garantizar de forma imparcial si el hecho jurídico a certificar ha cambiado o no.

En la etapa c), el método prevé, cuando la orden de activación ha sido seleccionada por parte del usuario, solicitar la toma por parte del usuario de al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico según diferentes valores de aumento para crear al menos un medio digital a certificar.

La etapa c) puede comprender una subetapa preliminar c0) de información por parte del usuario de un tamaño aproximado del hecho jurídico, siendo calculados los primeros, segundos y posiblemente terceros valores de aumento en función del tamaño aproximado del hecho jurídico.

En la etapa d), el método consiste en generar un fichero a certificar 106 que comprende dicho al menos un medio digital a certificar 105a, 105b, 105c, una hora de instantánea de dicho al menos un medio digital a certificar y coordenadas geográficas del aparato a la hora de la instantánea.

En la etapa e), si no puede establecerse una conexión a la red de telecomunicaciones, el método prevé almacenar temporalmente los medios digitales o el fichero a certificar 106 en la memoria dedicada inaccesible para el usuario durante una duración predeterminada y, si se puede establecer una conexión a la red de telecomunicaciones, transmitir el fichero a certificar (que contiene dicho al menos un medio digital a certificar) 106 al servidor de almacenamiento remoto por medio de la red de telecomunicaciones.

Entre la etapa e) y la etapa g), el método puede prever una etapa f) de comprobación de la conformidad del marcado único en dicho al menos un medio digital a certificar cuando el método prevea un marcado de este tipo en la etapa d).

En la etapa g), el método consiste en transmitir el fichero a certificar 106 que comprende dicho al menos un medio digital a certificar 105a, 105b, 105c a un tercero de confianza para su certificación.

La etapa g) puede comprender una subetapa preliminar g0) de selección del tercero de confianza entre una lista de terceros de confianza prerregistrados, de acuerdo con una regla de selección.

En una primera forma de realización alternativa V1, la etapa g) comprende una etapa g1) de transmisión a un tercero de confianza de un mensaje de advertencia de que un fichero a certificar 106 que comprende dicho al menos un medio digital a certificar 105a, 105b, 105c está presente en el servidor, una etapa g2) de visualización del medio digital a certificar en una interfaz del tercero de confianza cuando el tercero de confianza se conecta al servidor, y una etapa g3) de registro de un acta de certificación 114 en el servidor si el tercero de confianza certifica dicho al menos un medio digital a certificar, o de transmisión de una advertencia de no certificación al usuario si el tercero de confianza no certifica dicho al menos un medio digital a certificar.

En una segunda forma de realización alternativa V2, si el fichero a certificar 106 ha sido cifrado en la etapa d), la etapa g) comprende una etapa g'1) de transmisión a un tercero de confianza de una clave de descifrado y un mensaje de advertencia de que un fichero cifrado a certificar 106 que comprende dicho al menos un medio digital a certificar 106 está presente en el servidor, una etapa g'2) de descifrado y visualización del fichero descifrado a certificar en una interfaz del tercero de confianza, cuando el tercero de confianza se conecta al servidor, y una etapa g'3) de registro de un acta de certificación 114 en el servidor si el tercero de confianza certifica dicho al menos un medio digital a certificar, o de transmisión de una advertencia de no certificación al usuario si el tercero de confianza no certifica dicho al menos un medio digital a certificar.

En una tercera forma de realización alternativa V3, si el fichero a certificar 106 ha sido cifrado en la etapa d), la etapa g) comprende una etapa g"1) de transmisión del fichero cifrado a certificar que comprende dicho al menos un medio digital a certificar, sin clave de descifrado a un primer tercero de confianza custodio, una etapa g"2) de transmisión de la clave de descifrado del fichero cifrado a certificar, sin dicho fichero, a un segundo tercero de confianza custodio, una etapa g"3) de recogida, por parte de un tercero de confianza certificador, del fichero cifrado a certificar y de la clave de descifrado del primer y segundo terceros de confianza custodios respectivamente, una etapa g"4) de descifrado y visualización del fichero descifrado a certificar en una interfaz del tercero de confianza certificador cuando el tercero de confianza se conecta al servidor, y una etapa g"5) de registro en el servidor de un acta de certificación 114 si el tercero de confianza certificador certifica dicho al menos un medio digital a certificar, o de transmisión al usuario de una advertencia de no certificación si el tercero de confianza certificador no certifica dicho al menos un medio digital a certificar.

En la etapa h), el método consiste en emitir y registrar en el servidor un acta de certificación 114 si el medio digital está certificado (etapa hY)), o emitir y transmitir al usuario una advertencia de no certificación si el medio digital no está certificado (etapa hN)).

El método también puede incluir una etapa i) de cálculo de un retardo entre una hora de recepción del fichero a certificar 106 por parte del servidor remoto 101 y una hora de conexión del tercero de confianza al servidor de almacenamiento, y de comparación entre el retardo calculado y un periodo de reasignación predeterminado. La etapa i) también comprende la reasignación del fichero a certificar 106 a otro tercero de confianza si el retardo calculado excede el periodo de reasignación. Además, el método también puede prever que la etapa i) comprenda la emisión de una advertencia al usuario cuando el retardo calculado sea mayor que el periodo de reasignación predeterminado. De este modo, se advierte al usuario de que aún no ha sido posible certificar los medios.

El método también puede incluir una etapa j) de cálculo del tiempo transcurrido desde una hora de recepción del fichero a certificar 106 por parte del servidor de almacenamiento, de comparación del tiempo transcurrido desde la hora de recepción del fichero a certificar 106 por parte del servidor de almacenamiento con un retardo de respuesta predeterminado, y de emisión de un recordatorio al tercero de confianza cuando la hora de recepción del fichero a certificar 106 por parte del servidor de almacenamiento sea mayor que el retardo de respuesta predeterminado.

El método de certificación descrito en la invención permite realizar una certificación de alto valor probatorio de manera rápida, eficaz y totalmente digital (sin utilizar papel). Permite reducir el número de desplazamientos de las partes susceptibles de estar interesadas en el contenido del Acta (usuario, terceros de confianza, subcontratistas, autoridades locales, residentes, prensa, expertos), que ya no se tienen que desplazar hasta el lugar para ponerse de acuerdo sobre la realidad de un hecho. De esta forma, el método contribuye a reducir las emisiones de CO2 y a disminuir la huella de carbono de todas las partes implicadas.

REIVINDICACIONES

1. Método de certificación por parte de un tercero de confianza de medios digitales (105a, 105b, 105c) representativos de un hecho jurídico, capturados por un usuario (U) por medio de un aparato de captura de medios digitales (103), como por ejemplo, fotografías o vídeos, estando equipado el aparato (103) de una cámara digital, una biblioteca de almacenamiento nativo de medios digitales, una interfaz hombre/máquina (104) y un emisor/receptor que puede transmitir los medios digitales al menos a un servidor remoto (101) por medio de una red de telecomunicaciones (102), **caracterizándose** el método **por que** comprende las siguientes etapas:

a) crear una memoria dedicada en el aparato (103), diferente de la biblioteca nativa e inaccesible para el usuario, para procesar y/o almacenar los medios digitales a certificar, y prohibir el registro de medios digitales en la biblioteca nativa del aparato de captura;
b) mostrar una orden de activación en la interfaz (104) para iniciar una acción de certificación;
c) cuando la orden de activación ha sido seleccionada por parte del usuario, solicitar la toma de al menos una, preferiblemente al menos dos, ventajosamente al menos tres instantáneas del hecho jurídico por parte del usuario, para crear al menos un medio digital a certificar;
d) generar un fichero a certificar (106) que comprenda dicho al menos un medio digital a certificar (105a, 105b, 105c), una hora de instantánea de dicho al menos un medio digital a certificar y coordenadas geográficas del aparato a la hora de la instantánea;
e) si no se puede establecer una conexión a la red de telecomunicaciones, almacenar temporalmente el fichero a certificar (106) durante una duración predeterminada en la memoria dedicada inaccesible para el usuario y, si se puede establecer una conexión a la red de telecomunicaciones (102), transmitir el fichero a certificar (106) al servidor de almacenamiento remoto (101) por medio de la red de telecomunicaciones (102);
g) transmitir el fichero a certificar (106) que comprende dicho al menos un medio digital a certificar al tercero de confianza (120) para su certificación;
h) emitir y registrar en el servidor remoto (101) un acta de certificación (114) si dicho al menos un medio digital se certifica, o emitir y transmitir al usuario una advertencia de no certificación si dicho al menos un medio digital no se certifica.

2. Método de certificación de acuerdo con la reivindicación 1, en donde la etapa d) comprende además la estampación de un marcado único a dicho al menos un medio digital a certificar para crear al menos un medio digital marcado.

3. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 o 2, en donde la etapa g) comprende una etapa g1) de transmisión al tercero de confianza de un mensaje de advertencia de que un fichero a certificar que comprende dicho al menos un medio digital a certificar está presente en el servidor, una etapa g2) de visualización en una interfaz del tercero de confianza del medio digital a certificar cuando el tercero de confianza se conecta al servidor.

4. Un método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en donde la etapa d) comprende además cifrar el fichero a certificar y/o los medios digitales a certificar con una clave de cifrado, y la etapa g) comprende la transmisión al tercero de confianza una clave de descifrado.

5. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en donde el medio digital a certificar es del tipo fotografía, comprendiendo la etapa c) la toma de al menos dos, ventajosamente al menos tres, instantáneas del hecho jurídico por parte del usuario, desde un mismo ángulo de visión y según diferentes valores de aumento para crear al menos dos, preferiblemente al menos tres, fotografías digitales a certificar.

6. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en donde el medio digital a certificar es de tipo vídeo, comprendiendo la etapa c) la toma de multitud de instantáneas del hecho jurídico por parte del usuario según diferentes valores de aumento y eventualmente diferentes ángulos de visión, para crear al menos un vídeo digital a certificar.

7. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en donde las coordenadas geográficas del aparato registradas en la etapa d) se miden a la hora de cada instantánea y, a continuación, se procesan para obtener una posición geográfica media entre una primera instantánea y una última instantánea, registrándose esta posición geográfica media en el fichero a certificar.

8. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 7, en donde la etapa g) comprende una subetapa preliminar g0) de selección del tercero de confianza entre una lista de terceros de confianza prerregistrados, siendo la selección el resultado de una regla de selección que comprende la comparación de las coordenadas geográficas incluidas en el fichero a certificar con coordenadas geográficas representativas de cada tercero de confianza prerregistrado, y la selección de un tercero de confianza geográficamente más cercano a las coordenadas geográficas incluidas en el fichero a certificar.

9. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 8, en donde la etapa c) comprende medir automáticamente la distancia entre el aparato de captura de medios digitales y el hecho jurídico, y generar una señal de advertencia cuando el aparato se sitúa a una distancia predeterminada del hecho jurídico para permitir la

toma por parte del usuario de al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico, según diferentes valores de aumento.

10. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 9, en donde la etapa c) comprende una solicitud de una primera instantánea con un primer valor de aumento y, a continuación, una solicitud de una segunda instantánea con un segundo valor de aumento, diferente del primero y, a continuación, preferiblemente una solicitud de una tercera instantánea con un tercer valor de aumento, diferente del primero y del segundo, para permitir la toma por parte del usuario de al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico, según diferentes valores de aumento.

11. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 10, en donde la etapa c) comprende la captura de datos de distancia entre el aparato de captura y el hecho jurídico, y la etapa g) comprende el envío a una impresora 3D de datos de distancia y una orden para fabricar una reconstrucción tridimensional del hecho jurídico.

12. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 11, en donde la etapa e) comprende el registro de una hora de recepción del fichero a certificar por parte del servidor de almacenamiento, y la etapa g) comprende el registro de una hora de conexión del tercero de confianza al servidor de almacenamiento, comprendiendo el método de certificación, además, una etapa i) de cálculo de un retardo entre la hora de recepción del fichero a certificar por parte del servidor de almacenamiento y la hora de conexión del tercero de confianza al servidor de almacenamiento, de comparación del retardo calculado con un periodo de reasignación predeterminado, y de reasignación del fichero a certificar (106) a otro tercero de confianza.

13. Método de certificación de acuerdo con una cualquiera de las reivindicaciones 1 a 12, en donde la etapa e) comprende el registro de una hora de recepción del fichero a certificar por parte del servidor de almacenamiento, comprendiendo el método de certificación además una etapa j) de cálculo del tiempo transcurrido desde la hora de recepción del fichero a certificar por parte del servidor de almacenamiento, de comparación del tiempo transcurrido desde la hora de recepción del fichero a certificar por parte del servidor de almacenamiento y un retardo de respuesta predeterminado, y la emisión de un recordatorio al tercero de confianza cuando la hora de recepción del fichero a certificar por parte del servidor de almacenamiento sea mayor al retardo de respuesta predeterminado.

14. Sistema de certificación por un tercero de confianza de medios digitales representativos de un hecho jurídico, que comprende al menos un servidor remoto programado para comunicarse por medio de una red de telecomunicaciones con al menos un aparato de captura de medios digitales de un usuario, estando equipado el aparato de captura con una cámara digital, una biblioteca de almacenamiento nativo de los medios digitales capturados accesible por parte del usuario, una interfaz hombre-máquina, y un emisor/receptor que puede transmitir los medios digitales a dicho servidor remoto, **caracterizado por que**:

- el aparato de captura comprende una memoria dedicada separada de la biblioteca nativa, inaccesible para el usuario, para procesar y/o almacenar los medios digitales a certificar; y **por que**
- el aparato de captura y el servidor se programan para aplicar el método de acuerdo con una cualquiera de las reivindicaciones 1 a 13.

15. Sistema de certificación de acuerdo con la reivindicación 14, en donde el aparato de captura comprende además un sensor de distancia, estando programado el aparato para medir de forma automática una distancia entre el aparato de captura de medios digitales y el hecho jurídico, y para generar una señal de advertencia cuando el aparato esté situado a una distancia predeterminada del hecho jurídico para permitir la toma por parte del usuario de al menos dos, preferiblemente al menos tres, instantáneas del hecho jurídico según diferentes valores de aumento.

16. Sistema de certificación de acuerdo con la reivindicación 15 en donde el sensor de distancia se asocia a un sistema de barrido angular programado para efectuar un barrido de una zona definida que comprende el hecho jurídico y obtener una o más instantáneas constituidas por datos de distancia, estando programada el aparato de captura para producir una cartografía tridimensional de la superficie de dicha zona a partir de los datos de distancia obtenidos, y para generar un fichero a certificar que comprenda dicha cartografía como medio digital a certificar, un horario de obtención de la cartografía y coordenadas geográficas del aparato en el horario de la cartografía.

Fig. 1

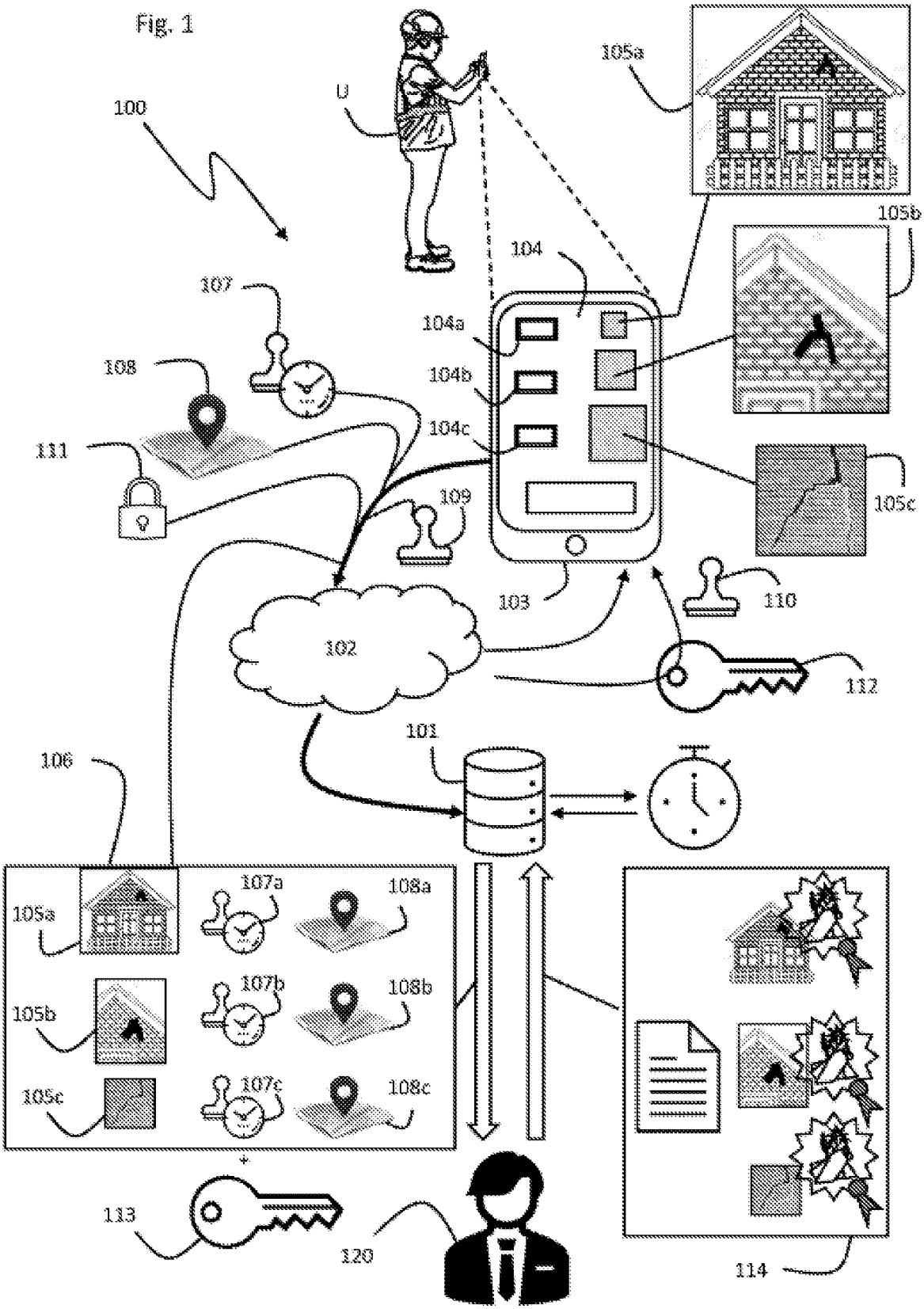
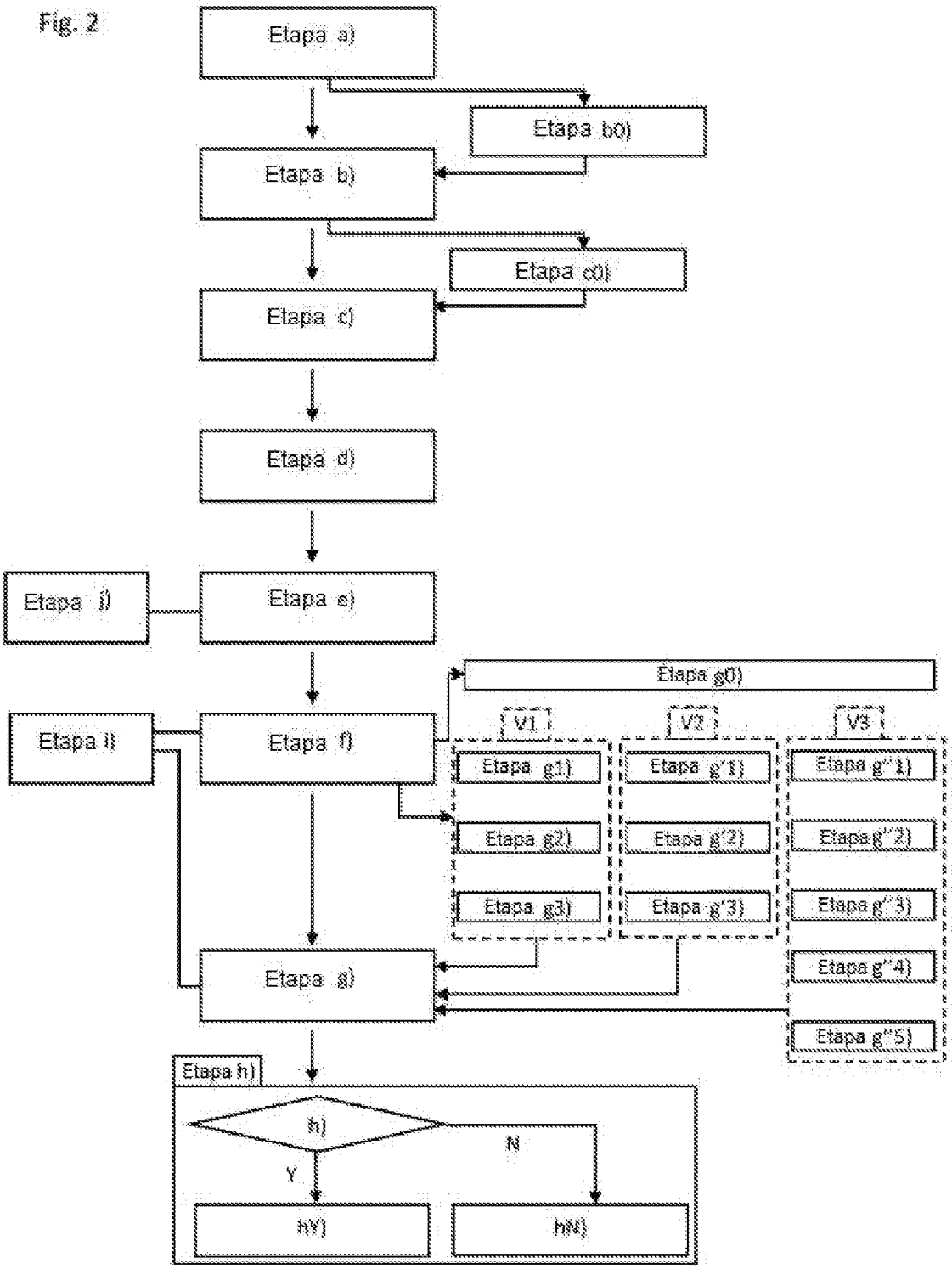

100
U
105a
105b
104
104a
104b
104c
105c
107
108
111
109
103
110
102
112
101
106
107a
108a
105a
107b
108b
105b
107c
108c
105c
113
120
114

Fig. 2


Etapa a)
Etapa b0)
Etapa b)
Etapa c0)
Etapa c)
Etapa d)
Etapa j)
Etapa e)
Etapa g0)
V1
V2
V3
Etapa i)
Etapa f)
Etapa g1)
Etapa g'1)
Etapa g''1)
Etapa g2)
Etapa g'2)
Etapa g''2)
Etapa g3)
Etapa g'3)
Etapa g''3)
Etapa g''4)
Etapa g)
Etapa g''5)
Etapa h)
h)
N
Y
hY)
hN)