(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 763 186**

(51) Int. CI.:

G06F 21/16 (2013.01)
G06F 21/64 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.03.2017 E 17382148 (9)**

(97) Fecha y número de publicación de la concesión europea: **23.10.2019 EP 3379440**

(54) Título: **Un método implementado en ordenador para certificar automáticamente documentos con garantías de integridad y autenticidad y programas de ordenador del mismo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.05.2020

(73) Titular/es:

TELEFONICA DIGITAL ESPAÑA, S.L.U. (100.0%)
Gran Vía 28
28013 Madrid, ES

(72) Inventor/es:

BIANZINO, ARUNA PREM;
TORRANO GIMÉNEZ, CARMEN;
SARWAT, RAMES y
SANCHEZ TABOADA, SALVADOR

(74) Agente/Representante:

ARIZTI ACHA, Monica

DESCRIPCIÓN

Un método implementado en ordenador para certificar automáticamente documentos con garantías de integridad y autenticidad y programas de ordenador del mismo

Campo de la invención

La presente invención se refiere en general a la autenticidad e integridad de documentos. En particular, la presente invención se refiere a un método implementado en ordenador, y también a programas de ordenador, para certificar automáticamente documentos con garantías de integridad y autenticidad.

Antecedentes de la invención

Cuando un usuario o una entidad está manejando un documento, sea en papel o en forma digital, se enfrenta a un problema común: verificar la autenticidad e integridad del documento. La autenticidad de un documento o certificado se refiere al hecho de que se haya emitido realmente por la entidad de emisión en la fecha establecida. Por otro lado, la integridad de un documento o certificado se refiere al hecho de que no haya sido editado después de su emisión (texto añadido/eliminado/alterado).

Actualmente se usan diferentes prácticas para comprobar si un documento es auténtico y no ha sido editado desde su emisión (es decir, la integridad). Todas ellas presentan limitaciones.

Los documentos pueden venir con un Código de Referencia Administrativo, por el que un servicio puede proporcionar la fecha de emisión del documento así como su remitente (para comprobar la autenticidad del documento) o la totalidad del documento (autenticidad e integridad). El último caso es proclive a la pérdida de datos, mientras que el primero no garantiza la integridad. Adicionalmente, en ambos casos, siempre es necesaria la intervención humana para comparar la fecha de emisión y/o el documento completo con el original, haciendo el sistema proclive a un error humano eventual.

Son conocidas algunas solicitudes de patente en el campo, por ejemplo:

El documento US-A1-20140049802 describe un sistema que se basa en la generación de una imagen codificada ETCODE usando técnicas esteganográficas, a ser impresa con el documento, usando impresoras convencionales. La decodificación se realiza mediante un dispositivo portátil de cámara digital, obteniendo por lo tanto la información oculta en ETCODE, y a continuación confrontada con la información acerca del documento en su versión digital presente en una base de datos. La solución descrita no se basa en un tercero de confianza ni describe cómo se realiza la comparación entre la copia presentada y la copia almacenada del documento y si está disponible o no tanto para documentos digitales como digitalizados.

El documento WO 2008108861 describe un método para procesamiento de documentos electrónicos, tal como facturas, especificaciones o contratos electrónicos, para asegurar la autenticidad, integridad, confidencialidad, y no repudio del documento. Se establece un proveedor de servicios tercero como el agente para las dos partes en interacción. El proveedor de servicios tercero recibe un documento electrónico de una primera parte, el documento electrónico relativo a la transacción entre las partes, siendo la transacción, por ejemplo, una venta o un contrato. El proveedor de servicios tercero proporciona una firma electrónica y certificación para el documento y archiva el documento, proporcionándole, junto con la certificación, a la segunda parte o a otros. La solución descrita solo funciona para documentos digitales y no para documentos digitalizados, para los que no ofrece ninguna garantía. Adicionalmente, la solución descansa en certificados digitales, sufriendo de las mismas limitaciones.

El documento KR 1020080014194 describe un sistema de repositorio de documentos electrónicos que incluye un módulo de autenticación, un módulo de registro, un módulo de lectura, un módulo de envío y un módulo de certificado. El módulo de autenticación se conecta a un terminal de usuario a través de una red, asegura la autenticidad de documentos electrónicos, realiza autenticación del usuario a través de un proceso de registro cuando un usuario accede al sistema de repositorio de documentos electrónicos. El módulo de registro comprueba un paquete de información del documento electrónico transmitido desde el usuario, genera metadatos, añade información de autenticación a los metadatos y almacena los metadatos en una base de datos. El módulo de lectura genera un paquete de información de lectura y transmite el paquete de información de lectura al usuario cuando el usuario desea leer un documento electrónico. El módulo de envío genera un paquete de información de envío y transmite el paquete al usuario cuando el usuario solicita al módulo de envío enviar un documento electrónico. El módulo de certificación envía un certificado para el documento electrónico o verifica un certificado enviado. Contrariamente a la presente invención, esta solución solo proporciona funcionalidades de envío y recuperación del documento, proporcionando documentos con metadatos embebidos para comprobación de la autenticidad en el lado del usuario, pero no permite comprobar automáticamente la autenticidad e integridad de un documento transportado: solo permite una comparación manual del documento transportado con la copia digital obtenida desde el repositorio,

para verificar la autenticidad e integridad del documento.

El documento US-A1-20090193259 describe una solución para almacenar documentos y comprobar su autenticidad. La solución descansa en un código de verificación del documento, fijado al documento en sí con una firma digital. La solución solo considera documentos digitales, y no los digitalizados. Más aún, esta solución incluye la síntesis del código de verificación en una forma visible en el interior del documento, y no en una forma inapreciable tal como se describe en la presente invención. Adicionalmente, la solución no permite la inclusión de metadatos en el documento, sino solo un código de verificación del documento en sí. Adicionalmente, no se divulgan detalles sobre cómo se calcula el código de verificación del documento, o cómo se almacenan los documentos en una forma inalterable.

El documento US-A1-20100122348 A1 describe una solución para digitalizar documentos y almacenarlos en un repositorio para comprobar su autenticidad basándose en una marca aplicada a la versión digital. La marca es una combinación del remitente y de marcas almacenadas. Contrariamente a la presente invención, esta solución solo considera documentos digitalizados y no los nativos digitales. La solución descrita incluye una marca visible en el documento. Como tal, solo garantiza la integridad del documento en una comparación manual. Adicionalmente, la marca incluida no permite almacenamiento de metadatos. Finalmente, no se divulgan detalles sobre cómo se almacena un documento en una forma inalterable en el lado de almacenamiento.

Alain Brenzikofers “Libro blanco de marca de tiempo de confianza descentralizada”, (Recuperado de Internet: URL: https: //www.scs.ch/blog/wp-content/uploads/ 2017/01/trusted-sensor-whitepaper.pdf) da a conocer un método para la marca de tiempo descentralizada de documentos en una cadena de bloques del libro mayor distribuido para la prueba de existencia combinada con la marca de agua del documento con una síntesis del último bloque para la prueba de inexistencia previa.

"Esquema de marca de agua frágil basado en cadena de bloques con localización superior", (19 de mayo de 2008, NETWORK Y PARALLEL COMPUTING; SPRINGE, PÁGINA (S) 147 - 160) de HE HONG-JIE *ET AL* da a conocer otro método para la marca de agua de imágenes digitales usando cadena de cloques para proporcionar integridad y autenticidad.

Son necesarias por lo tanto más soluciones para asegurar la integridad y autenticidad y también prueba de la existencia de documentos o certificados digitales o digitalizados.

Descripción de la invención

Realizaciones de la presente invención proporcionan de acuerdo con un aspecto, un método implementado en ordenador para certificar automáticamente documentos con garantías de integridad y autenticidad, el método comprende primero la recepción, por un segundo sistema de ordenador, desde un primer sistema de ordenador (remitente), de al menos un documento (un documento digital, por ejemplo, un PDF) a ser certificado, estando identificado el al menos un documento en el segundo sistema de ordenador con metadatos que incluyen al menos un identificador del primer sistema de ordenador y una marca de tiempo. A continuación, el segundo sistema de ordenador calcula una primera función criptográfica (como por ejemplo una función de código de verificación) del documento recibido y envía la primera función criptográfica calculada a un tercer sistema de ordenador mantenido dentro de un medio de registro distribuido tal como un DLT, almacenando el tercer sistema de ordenador la primera función criptográfica en la menos una memoria del mismo. A continuación, el segundo sistema de ordenador recibe una primera síntesis de mensaje que corresponde a un identificador de que se ha almacenado la primera función criptográfica en el tercer sistema de ordenador. A continuación, en el método propuesto, el segundo sistema de ordenador calcula una clave usando la primera síntesis de mensaje recibido y dichos metadatos del documento, siendo decodificada dicha clave calculada en una marca de agua (es decir, una alteración del documento que puede incluir una imagen de identificación o plantilla, tal como espaciado de caracteres o deformación de los caracteres en el caso de texto, o desplazamiento de píxeles en la frecuencia o el espacio en el caso de imágenes) que se aplica al documento proporcionando un documento modificado. El documento modificado se envía por el segundo sistema de ordenador al primer sistema de ordenador para ser almacenado. El segundo sistema de ordenador calcula a continuación una segunda función criptográfica del documento modificado y envía la segunda función criptográfica calculada y el documento modificado al tercer sistema de ordenador para almacenamiento del mismo. Finalmente, el segundo sistema de ordenador recibe una segunda síntesis de mensaje que corresponde a un identificador de haber almacenado la segunda función criptográfica en el tercer sistema de ordenador, y lo almacena localmente.

Por DLT se ha de entender un consenso de datos digitales replicados, compartidos y sincronizados, geográficamente dispersos a través de múltiples sitios, países o instituciones. No hay un administrador central o almacenamiento de datos centralizado. En consecuencia, el sistema resultante es tolerante a fallos y universal (es decir, puede adoptarse independientemente de la localización geográfica). Se requiere una red entre iguales así como algoritmos de consenso para asegurar que se emprende la réplica a través de los nodos. Una cadena de Bloques es una posible implementación del DLT.

De acuerdo con una realización, la marca de agua se replica en diferentes puntos del documento modificado permitiendo por ello comprobar la autenticidad del documento o incluso la autenticidad de una parte del documento, si se ha dañado (es decir, un documento roto en donde se pierde una parte, o un documento en papel sucio/arrugado, etc.). Preferentemente, la marca de agua se configura para ser indistinguible al ojo humano, mientras que puede identificarse en una inspección digital.

De acuerdo con el método propuesto, el documento modificado puede enviarse, por el primer sistema de ordenador, a un usuario después de que este último haya sido válidamente autenticado.

De acuerdo con una primera realización, el segundo sistema de ordenador recibe un documento digital desde el usuario y adicionalmente extrae la marca de agua del documento digital recibido y decodifica la clave a partir de ella, y recupera la segunda función criptográfica desde el tercer sistema de ordenador proporcionando a este último la segunda síntesis de mensaje.

A continuación, el segundo sistema de ordenador extrae los metadatos del documento a partir de la clave, calcula la tercera función criptográfica del documento digital y compara la tercera función criptográfica con la segunda función criptográfica que ha recuperado del tercer ordenador servidor. Finalmente, el segundo sistema de ordenador informa al usuario de un resultado de dicha comparación y también envía los metadatos a este último.

La recuperación de la segunda función criptográfica y la extracción de los metadatos pueden realizarse al mismo tiempo.

De acuerdo con una segunda realización, el segundo sistema de ordenador recibe un documento digitalizado (por ejemplo, un escaneado/ imagen del documento digital previamente impreso en papel o la conversión a un formato digital diferente de un documento digital) desde el usuario y extrae adicionalmente la marca de agua del documento digitalizado recibido decodificando a partir de ella la clave. A continuación, el segundo sistema de ordenador extrae los metadatos del documento, incluyendo el identificador del primer sistema de ordenador y la marca de tiempo a partir de la clave, y la primera síntesis de mensaje a partir de la clave, y usa la primera síntesis de mensaje para recuperar la primera función criptográfica desde el tercer sistema de ordenador para comprobar la existencia y registro del documento. Finalmente, el segundo sistema de ordenador envía una respuesta al usuario acerca de la existencia y registro del documento en el tercer sistema de ordenador y los metadatos extraídos para una comprobación de autenticidad adicional por parte del usuario.

La extracción de los metadatos y la extracción de la primera síntesis de mensaje pueden realizarse al mismo tiempo.

De acuerdo con una tercera realización, el segundo sistema de ordenador autentica la información de identificación del usuario y después de que se confirme dicha autenticación el segundo sistema de ordenador recibe un documento digitalizado desde el usuario. A continuación, el segundo sistema de ordenador extrae la marca de agua del documento digitalizado recibido y decodifica a partir de ella la clave, usando la segunda síntesis de mensaje para recuperar el documento modificado desde el tercer sistema de ordenador. A continuación, el segundo sistema de ordenador, extrae los metadatos del documento digital recibido incluyendo el identificador del primer sistema de ordenador y la marca de tiempos a partir de la clave. Finalmente, el segundo sistema de ordenador, envía al usuario los metadatos extraídos de modo que pueda verificar la autenticidad del documento, y también le envía el documento recuperado de modo que pueda comprobar su integridad.

Otras realizaciones de la invención que se divulgan en el presente documento incluyen programas de software para realizar las etapas de realización del método y operaciones resumidas anteriormente y divulgadas en detalle a continuación. Más particularmente, un producto de programa de ordenador es una realización que tiene un medio legible por ordenador que incluye instrucciones de programa de ordenador codificadas en él que cuando se ejecutan en al menos un procesador en un sistema de ordenador hace que el procesador realice las operaciones indicadas en el presente documento como realizaciones de la invención.

La presente invención garantiza:

- Integridad del documento, es decir, garantiza que un documento no se ha alterado desde su emisión;

- Autenticidad del documento, significando que el origen de un documento puede ser identificado unívocamente;

- Prueba de existencia, significando que es posible identificar la referencia de tiempos de cuándo existió el documento;

- No repudio en origen, significando que el remitente de un documento no puede repudiar que es el

originador de dicho documento;

- Confidencialidad, es decir, solo el remitente y el receptor pueden acceder al documento original tal como está almacenado en el repositorio, después de una autenticación con éxito (en tanto que cualquier usuario que transporte el documento puede acceder a la autenticidad y prueba de existencia acerca del documento transportado). Adicionalmente, la marca de agua aplicada no es apreciable en inspección humana, dando como resultado por tanto seguridad con respecto a observadores externos y errores humanos en la transcripción a diferencia del Código de Referencia Administrativo, por ejemplo, que es visible y por lo tanto inseguro;

- Robustez, significando que las garantías anteriores permanecen también en caso de documentos dañados, o parciales, así como tanto en caso de documentos digitales como digitalizados.

Adicionalmente, las garantías proporcionadas se basan en una infraestructura de medio de registro distribuido, siendo por tanto:

- Perdurable, significando que la información almacenada no puede editarse o borrarse con el tiempo:

- Robusto: dado que la infraestructura está distribuida, el resultado es tolerante a fallos;

- Universal, significando que puede ser accedido independientemente de la localización geográfica.

Finalmente, la presente invención se basa en una tercera parte de confianza, garantizando por ello:

- Neutralidad con respecto al almacenamiento y características del documento.

- Accesibilidad, significando que la solución es accesible también por remitentes privados y no solo por administraciones públicas que la implementen.

Breve descripción de los dibujos

Las anteriores y otras ventajas y características se entenderán más completamente a partir de la siguiente descripción detallada de realizaciones, con referencia a los dibujos adjuntos, que deben considerarse en una forma ilustrativa y no limitativa, en los que:

la Fig. 1 es un diagrama de secuencia de registro del documento por parte de un remitente o el primer sistema de ordenador.

La Fig. 2 es un diagrama de secuencia de la comprobación de integridad y autenticidad por un usuario para un documento digital.

La Fig. 3 es un diagrama de secuencia de la comprobación de autenticidad por un usuario para un documento digitalizado.

La Fig. 4 es un diagrama de secuencia de la comprobación de integridad y autenticidad por un usuario para un documento digitalizado.

Descripción detallada de la invención

La presente invención permite garantizar la integridad y autenticidad del documento en una forma automática y en tiempo real, mientras que también garantiza la prueba de existencia en el tiempo del documento comprobado, el no repudio del remitente del documento, la confidencialidad del documento, un acceso universal a la solución, en espacio y tiempo, neutralidad de la solución con respecto al remitente y usuario, y la robustez de la solución para documentos dañados.

Cuando un documento es emitido por un remitente autorizado (o primer sistema de ordenador como se denomina en las reivindicaciones) 10, es decir, una entidad (privada o pública) autorizada para emitir documentos y almacenarlos usando el método propuesto, (Fig. 1), antes de que se entregue al usuario final 1; el remitente 10 registra el documento en el sistema objetivo. Como una primera etapa para registro del documento, el remitente 10 envía el documento original al sistema 20 objetivo (o segundo sistema de ordenador como se denomina en las reivindicaciones). Solamente remitentes autorizados pueden enviar documentos al sistema 20 objetivo. Su autorización es garantizada por un sistema de autenticación apropiado. La limitación del remitente 10 impide la emisión de documentos falsos de parte de otros remitentes, mientras que la naturaleza perdurable e inalterable de un sistema de medio de registro distribuido tal como un DLT 30 garantiza la prueba de existencia del documento y el no repudio del mismo en el lado del remitente 10.

Una vez es recibido un documento original D_0 por el sistema 20 objetivo, se calcula una primera función criptográfica tal como una función de código de verificación h_0 del documento y se almacena en el DLT 30. Cada vez que la primera función criptográfica se almacena en un DLT 30, se devuelve una primera síntesis (código de verificación del registro – h_{R0}). La primera síntesis devuelto se combina con el identificador del remitente 10, la marca de tiempos y otros métodos eventuales para crear una clave K, que se decodifica en una marca de agua para ser aplicada al documento original así como para futuras comprobaciones sobre la autenticidad del documento. El documento obtenido después de la aplicación de la marca de agua D_W (es decir, el documento modificado) se devuelve al remitente 10 para ser entregado al usuario final 1. Adicionalmente, se calcula una segunda función de criptográfica tal como una función de código de verificación del documento modificado D_W, y se almacena en el DLT 30 para futuras comprobaciones de integridad, junto con el documento modificado D_W en sí mismo.

De acuerdo con el método propuesto, la marca de agua aplicada al documento consiste en una marca de agua especial que representa un código (clave K) y replicada en diferentes puntos del documento en sí, permitiendo por ello la comprobación de la autenticidad del documento o incluso la autenticidad de una parte del documento, si se ha dañado. La marca de agua, adicionalmente, no puede apreciarse por una inspección humana, garantizando por ello la seguridad contra observadores externos, así como la robustez frente a errores humanos.

Cualquier usuario final 1 puede, de acuerdo con una primera realización, verificar en cualquier momento la autenticidad e integridad de un documento digital en su posesión - siempre que el documento original se haya registrado usando la solución descrita - mediante el envío al sistema objetivo descrito 20 (Fig. 2). Cuando se recibe un documento digital D_X por el sistema 20 objetivo, este último extrae la marca de agua del documento D_X recibido y decodifica a partir de ella la clave K. Entonces se usa la síntesis de la segunda función criptográfica para recuperar desde el DLT 30 la segunda función criptográfica h_w del documento depositado por el remitente 10. Preferentemente, al mismo tiempo, se extraen los metadatos del documento a partir de la clave K. Se calcula una tercera función criptográfica tal como una función de código de verificación h_x del documento recibido por parte del sistema 20 objetivo y se contrasta contra la segunda función criptográfica h_w almacenada. Si el contraste es positivo (es decir, si son iguales), se devuelve una respuesta positiva de autenticidad e integridad del documento al usuario final 1, en caso contrario se devuelve una respuesta negativa. Adicionalmente, se devuelven metadatos acerca del documento y del remitente 10 al usuario final 1.

De una forma similar, cualquier usuario final puede, de acuerdo con una segunda realización, verificar en cualquier momento la autenticidad de un papel o documento digitalizado (foto, escáner, conversión de formato) - siempre que el documento original se halla registrado usando el sistema 20 objetivo descrito - mediante el envío del documento digitalizado a este último (Fig. 3). Cuando se recibe un documento D_y digitalizado por el sistema 20 objetivo, este último extrae la marca de agua de él y decodifica a partir de ella la clave K. A continuación se extraen los metadatos del documento a partir de la clave, incluyendo el identificador del remitente, marca de tiempo de registro y eventualmente otros metadatos incluidos en el momento del registro del documento original D_0. Preferentemente, al mismo tiempo, se extrae la primera síntesis h_{R0} a partir de la clave K. Junto a ello, se usa la primera síntesis h_{R0} para recuperar la primera función criptográfica h_o del tercer sistema 30 de ordenador para comprobar la existencia y registro del documento. Los metadatos obtenidos se devuelven a continuación al usuario final 1 para comprobación de autenticidad de la identidad del remitente 10, marca de tiempos de envío y eventualmente otros apartados de comprobación incluidos. Esta segunda comprobación en el lado del usuario evita la posibilidad de reutilización de una síntesis original válida h_{R0} sobre documentos falsos.

Cualquier usuario final puede también, de acuerdo con una tercera realización, obtener el documento modificado y verificar en cualquier momento la autenticidad e integridad de un papel o documento digitalizado (foto, escáner, conversión de formato) (Fig. 4) —siempre que el documento original se haya registrado usando la solución descrita— mediante la autenticación en el sistema 20 objetivo. La autenticación del usuario 1 puede basarse en una cadena de caracteres de identificación personal (contraseña), una clave de seguridad, mantenimiento del teléfono móvil (incluyendo restricciones eventuales para la autenticación del usuario en base a la localización geográfica del teléfono móvil), o en una combinación de más de uno de los factores de autenticación listados. Una vez se ha confirmado la autenticación por el servicio objetivo 20, el usuario final 1 envía el documento digitalizado D_y al sistema 20 objetivo. A continuación el sistema 20 objetivo extrae la clave de la marca de agua K desde él y la traduce en la clave K. A continuación se usa la segunda síntesis de mensaje h_{rw} para recuperar del DLT 30 el documento D_W modificado registrado, adicionalmente, se extraen los metadatos disponibles a partir de la clave K incluyendo el identificador del remitente, marca de tiempo de registro y otros metadatos eventuales incluidos en el momento del registro del documento original D_0. Finalmente, los metadatos obtenidos se devuelven al usuario final 1 para comprobación de autenticidad, y el documento con la marca de agua D_W se devuelve al usuario final 1 para comprobación de integridad del documento digitalizado.

El servicio descrito se implementa en una organización independiente tanto del remitente 10 como del usuario final 1, garantizando la neutralidad en este sentido y constituyendo una tercera parte de confianza, accesible por cualquier remitente (siendo este privado o público) y por cualquier usuario.

Mientras que lo anterior se ha dirigido a realizaciones de la presente invención, pueden concebirse realizaciones distintas y adicionales de la invención sin apartarse del alcance básico de la misma. Por ejemplo, pueden implementarse otros aspectos en hardware o software o en una combinación de hardware y software.

Adicionalmente, los programas de software incluidos como parte de la invención pueden realizarse en un producto de programa de ordenador que incluye un medio utilizable por ordenador. Por ejemplo, dicho medio utilizable por ordenador puede incluir un dispositivo de memoria legible, tal como un dispositivo de disco duro, un dispositivo de memoria flash, un CD-ROM, un DVD/ROM, o un disquete de ordenador que tenga segmentos del código de programa legible por ordenador almacenados en él. El medio legible por ordenador puede incluir también un enlace de comunicaciones, tanto óptico, como por cable, o inalámbrico, que tenga segmentos de código de programa transportados sobre él como señales digitales o analógicas.

El alcance de la presente invención se determina por las reivindicaciones que siguen.

REIVINDICACIONES

1. Método implementado en ordenador para certificar automáticamente documentos con garantías de integridad y autenticidad, comprendiendo el método:

- recibir, por un segundo sistema (20) de ordenador, desde un primer sistema (10) de ordenador, al menos un documento (D_o) a ser certificado, estando identificado el al menos un documento (D_o) en el segundo sistema (20) de ordenador con metadatos que incluyen al menos un identificador del primer sistema (10) de ordenador y una marca de tiempo;

- calcular, por el segundo sistema (20) de ordenador, una primera función (h_o) criptográfica del documento (D_o) recibido;

- enviar, por el segundo sistema (20) de ordenador, la primera función (h_o) criptográfica calculada a un tercer sistema (30) de ordenador mantenido dentro de un medio de registro distribuido, almacenando el tercer sistema (30) de ordenador la primera función (h_o) criptográfica en al menos una memoria del mismo;

- recibir, por el segundo sistema (20) de ordenador, una primera síntesis (h_{ro}) de mensaje que corresponde a un identificador de haber almacenado la primera función (h_o) criptográfica en el tercer sistema (30) de ordenador;

- calcular, por el segundo sistema (20) de ordenador, una clave (K) que usa la primera síntesis (h_{ro}) de mensaje recibido y dichos metadatos del documento (D_o), siendo decodificada dicha clave calculada (K) en una marca de agua que se aplica al documento (D_o) proporcionando un documento (D_W) modificado;

- enviar, por el segundo sistema (20) de ordenador, el documento (D_W) modificado al primer sistema (10) de ordenador;

- calcular, por el segundo sistema (20) de ordenador, una segunda función (h_w) criptográfica del documento (D_W) modificado, y enviar la segunda función (h_w) criptográfica calculada y el documento (D_W) modificado al tercer sistema (30) de ordenador para almacenamiento del mismo;

- recibir, por el segundo sistema (20) de ordenador, una segunda síntesis (h_{rw}) de mensaje que corresponde a un identificador de haber almacenado la segunda función (h_w) criptográfica en el tercer sistema (30) de ordenador, y almacenar dicha segunda síntesis (h_{rw}) de mensaje localmente en el segundo sistema (20) de ordenador; y

- enviar, mediante el primer sistema (10) de ordenador, el documento modificado (D_W) a un usuario (1) después de que el usuario (1) haya sido autenticado válidamente,

en el que el segundo sistema (20) de ordenador recibe adicionalmente un documento (D_X) digital o (D_y) digitalizado desde el usuario (1), en el que

- si se recibe un documento (D_x) digital, el segundo sistema (20) de ordenador adicionalmente:

- extrae la marca de agua desde el documento (D_X) digital recibido y decodifica a partir de ella la clave (K) y recupera la segunda función (h_w) criptográfica desde el tercer sistema (30) de ordenador proporcionando este último la segunda síntesis (h_{rw}) de mensaje;

- extrae los metadatos del documento (D_o) a partir de la clave (K);

- calcula una tercera función (h_x) criptográfica del documento (D_X) digital y compara la tercera función (h_x) criptográfica con la segunda función (h_w) criptográfica que se ha recuperado desde el tercer servidor (30) de ordenador; e

- informa de un resultado de dicha comparación al usuario (1) y también envía metadatos a este último, o

- si se recibe un documento (D_y) digitalizado, el segundo sistema (20) de ordenador adicionalmente:

- extrae la marca de agua desde el documento (D_y) digitalizado recibido y decodifica a partir de ella la clave (K);

- extrae los metadatos del documento (D_o) incluyendo el identificador del primer sistema (10) de ordenador y la marca de tiempo a partir de la clave (K), y la primera síntesis (h_{ro}) de mensaje a partir de la clave (K), y

usa la primera síntesis (h_{ro}) de mensaje para recuperar la primera función (h_o) criptográfica desde el tercer sistema (30) de ordenador para comprobar la existencia y registro del documento; y

- envía una respuesta acerca de la existencia y registro del documento en el tercer sistema (30) de ordenador y los metadatos extraídos para comprobación de autenticidad adicional por parte del usuario (1); o

- si se recibe un documento (D_y) digitalizado, antes de recibir, el segundo sistema (20) de ordenador autentica la información de identificación del usuario (1) y después de que se confirme la autenticación, y el documento (D_y) digitalizado recibido, el segundo sistema (20) de ordenador adicionalmente:

- extrae la marca de agua desde el documento (D_y) digitalizado recibido y decodifica a partir de ella la clave (K) y usa la segunda síntesis (h_{rw}) de mensaje para recuperar el documento (D_W) modificado desde el tercer sistema (30) de ordenador;

- extrae los metadatos que incluyen el identificador del primer sistema (10) de ordenador y la marca de tiempo desde la clave (K); y

-envía los metadatos extraídos al usuario (1) de modo que pueda verificar la autenticidad del documento, y envía el documento (D_W) modificado recuperado al usuario (1) de modo que pueda comprobar su integridad.

2. Método según la reivindicación 1, en el que la marca de agua se replica en diferentes puntos del documento (D_w) modificado.

3. Método según la reivindicación 2, en el que dicha marca de agua se configura para ser indistinguible para el ojo humano.

4. Método según las reivindicaciones previas, en el que el documento (D_o) es un documento digital.

5. Método según la reivindicación 1, en el que la recuperación de la segunda función (h_w) criptográfica y la extracción de los metadatos se realizan al mismo tiempo.

6. Método según la reivindicación 1, en el que si se recibe un documento (Dy) digitalizado, la extracción de los metadatos y la extracción de la primera síntesis (hro) de mensaje se realizan al mismo tiempo.

7. Medio legible por ordenador no transitorio que comprende instrucciones de código que cuando se ejecutan en al menos un procesador de un sistema de ordenador implementan el método de cualquiera de las reivindicaciones 1 a 6.

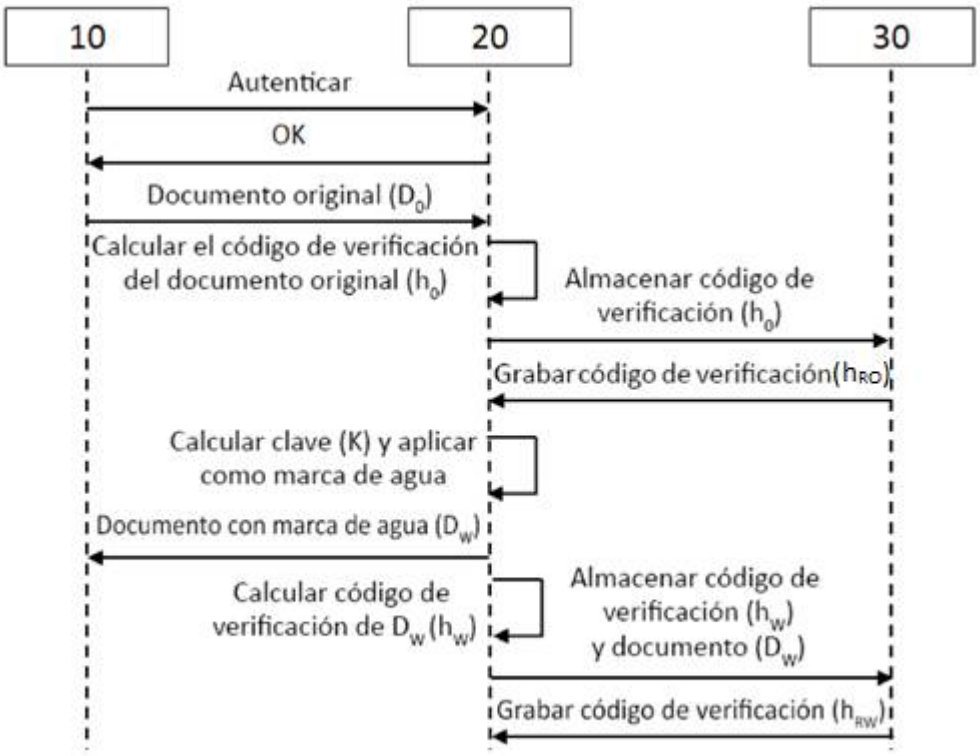
10
20
30
Autenticar
OK
Documento original (D_0)
Calcular el código de verificación del documento original (h_0)
Almacenar código de verificación (h_0)
Grabar código de verificación (h_{RO})
Calcular clave (K) y aplicar como marca de agua
Documento con marca de agua (D_W)
Calcular código de verificación de D_W (h_W)
Almacenar código de verificación (h_W) y documento (D_W)
Grabar código de verificación (h_{RW})

Fig. 1

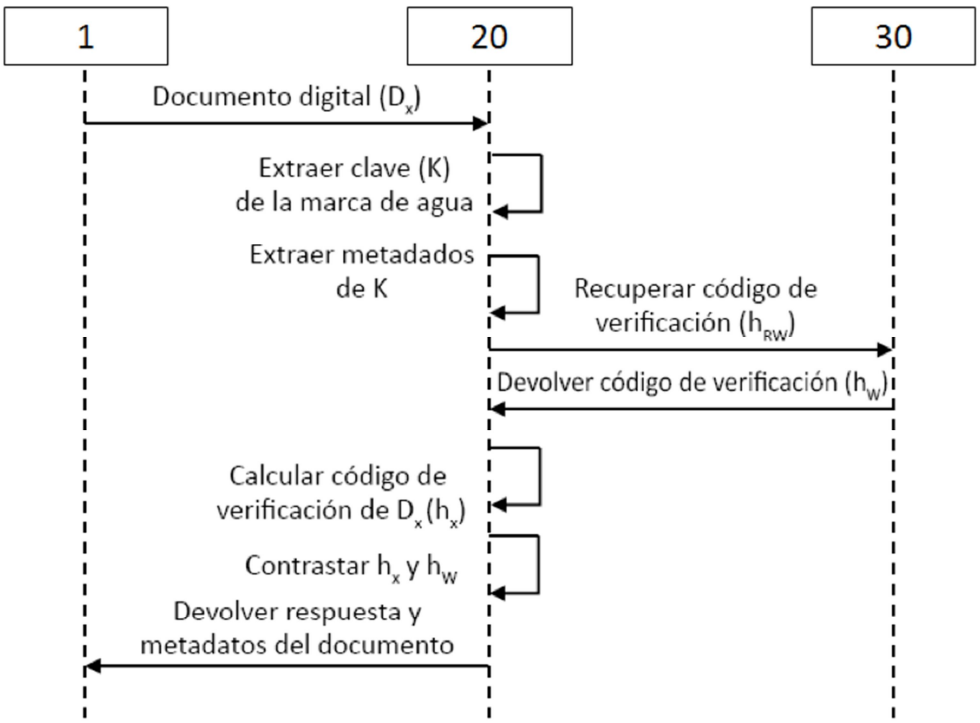
1
20
30
Documento digital (D_x)
Extraer clave (K) de la marca de agua
Extraer metadados de K
Recuperar código de verificación (h_{RW})
Devolver código de verificación (h_W)
Calcular código de verificación de D_x (h_x)
Contrastar h_x y h_W
Devolver respuesta y metadatos del documento

Fig. 2

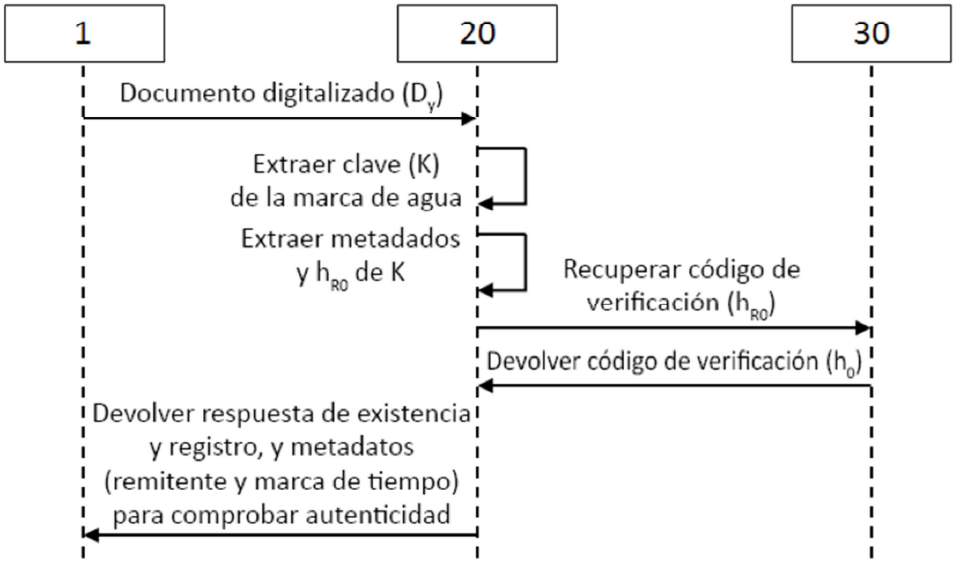
1
20
30
Documento digitalizado (D_y)
Extraer clave (K) de la marca de agua
Extraer metadados y h_{R0} de K
Recuperar código de verificación (h_{R0})
Devolver código de verificación (h_0)
Devolver respuesta de existencia y registro, y metadatos (remitente y marca de tiempo) para comprobar autenticidad

Fig. 3

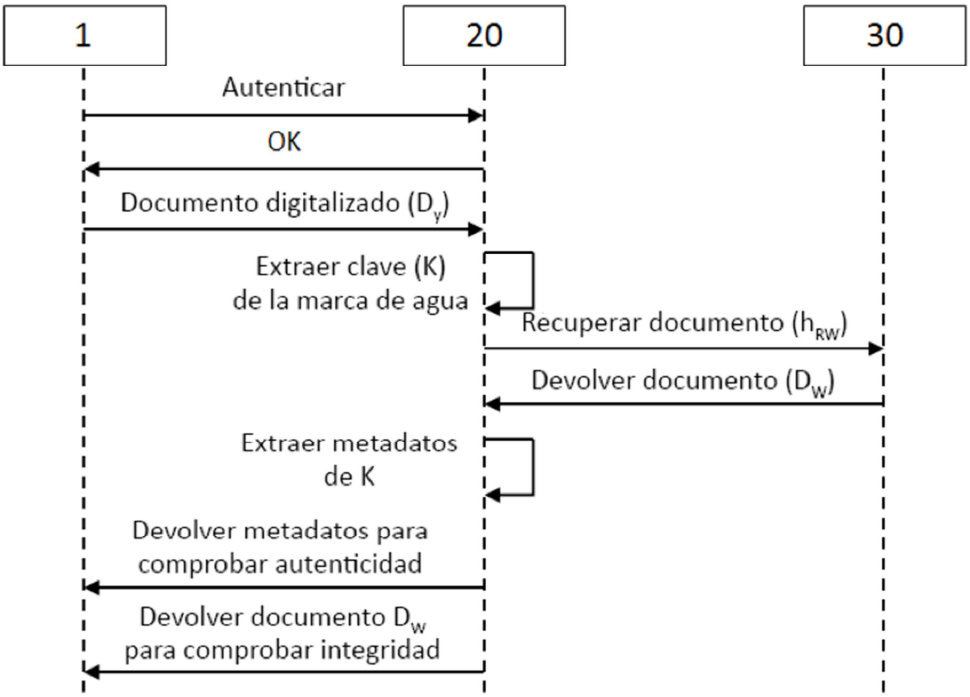
1
20
30
Autenticar
OK
Documento digitalizado (D_y)
Extraer clave (K)
de la marca de agua
Recuperar documento (h_{RW})
Devolver documento (D_W)
Extraer metadatos
de K
Devolver metadatos para
comprobar autenticidad
Devolver documento D_W
para comprobar integridad

Fig. 4