(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 716 308**

(21) Número de solicitud: 201731397

(51) Int. CI.:

H04L 9/00 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

11.12.2017

(43) Fecha de publicación de la solicitud:

11.06.2019

(71) Solicitantes:

DÍAZ BAÑO, Pablo (100.0%)
Gran Vía de les Corts Catalanes 1069, 5º, 4ª
08020 Barcelona ES

(72) Inventor/es:

DÍAZ BAÑO, Pablo

(54) Título: **Método para autenticar una firma dinámica con el documento firmado mediante una firma electrónica.**

(57) Resumen:

Método para autenticar una firma dinámica con el documento firmado mediante una firma electrónica.
Esta divulgación se refiere a un método que captura el grafo y la firma digitalizada de una firma autógrafa, y mediante la aplicación de un algoritmo de digestión sobre esos valores, se obtiene un hash que es firmado electrónicamente por un segundo usuario que emplea un certificado y un dispositivo de creación de firma de criptografía de clave pública. Este método asocia de forma ineludible el documento y la firma manuscrita electrónica y garantiza su integridad.

ES 2 716 308 A1

D E S C R I P C I Ó N

MÉTODO PARA AUTENTICAR UNA FIRMA DINÁMICA CON EL DOCUMENTO FIRMADO MEDIANTE UNA FIRMA ELECTRÓNICA

SECTOR DE LA TÉCNICA

La presente invención pertenece al sector de la seguridad de documentos electrónicos.

Se refiere a un nuevo procedimiento que realiza una firma autógrafa sobre una pizarra digital para adherirse a un determinado documento electrónico, y tras capturar el grafo y la imagen digitalizada, se genera un hash del documento electrónico y del archivo que contiene los datos capturados de la firma autógrafa; el hash es firmado electrónicamente empleando un certificado de firma electrónica de criptografía de clave pública. De esta forma el documento y la firma manuscrita electrónica quedan ineludiblemente asociados y su integridad garantizada.

ANTECEDENTES DE LA INVENCIÓN

Las pizarras digitales, también conocidas como Tablet se han popularizado en los últimos años y están siendo utilizadas para otorgar todo tipo de consentimientos firmados, desde la recepción de un paquete hasta un ingreso bancario.

No obstante, al contrario de la creencia popular, la realidad es que la firma autógrafa con la que el firmante expresa su consentimiento sobre el contenido de un documento electrónico no se estampa sobre él, ni tan siquiera queda ligada a él. Por lo tanto, es perfectamente posible asociar esa firma manuscrita electrónica a otro documento completamente distinto al que el firmante tuvo la voluntad de aceptar, y sin que sea posible detectar esa sustitución.

Esta debilidad que padece la técnica de la “firma manuscrita electrónica” también denominada “firma dinámica” es conocida, y muchos de los sistemas que se comercializan en el mercado, intentan resolver está debilidad enviando el archivo que contiene los valores de la firma manuscrita electrónica y el archivo del documento electrónico a un servidor remoto que se encarga de asociarlos, bien aplicando un cifrado

de clave pública o incluso elaborando una firma electrónica. Ningún procedimiento existente tiene en cuenta la presencia de una segunda persona, que es la que siempre hace cesión de uso de la pizarra digital y en cuya presencia el firmante elabora su firma autógrafa como expresión de voluntad de aceptación del contenido del documento. La novedad de esta invención es desarrollar un ingenioso método en el que se incluye en el sistema dos elementos de alta seguridad como son el dispositivo de firma electrónica de criptografía de clave pública y el certificado de firma electrónica, de esta forma, el sujeto que hasta ahora era mero cesionario de una pizarra electrónica, al ser dotado de esta tecnología y estar presente en el acto de la firma, interviene en el mismo acto como testigo, autenticando la firma autógrafa, asociándola de forma indisoluble al documento electrónico e incluso, constando su presencia como testigo al estar su identidad reseñada en el certificado electrónico empleado conforme al estándar X509 v3.

Existe extensa documentación que describe sistemas de firma electrónica basada en criptografía de clave pública, generación y uso de los certificados de firma electrónica. En la actualidad estos instrumentos son de uso común y hay innumerables aplicaciones de código fuente abierto que permite implementar el método propuesto en esta invención. Las normas técnicas de referencia son: ETSI TS 101 733, v.1.6.3, v1.7.4 y v.1.8.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES); ETSI TS 101 903, v.1.2.2, v.1.3.2 y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES); ETSI TS 102 778, v 1.2.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic - Profile based on ISO 32000-1, Part 3: PAdES Enhanced - PAdES-BES and PAdESEPES Profiles; Part 4: Long-term validation. RFC 5280 (X509 v3).

La firma dinámica también conocida como firma manuscrita electrónica o firma biométrica, esta extensamente documentada y los modelos habitualmente utilizados están detalladamente descritos en las normas técnicas: ISO / IEC 19794-7: 2014 Formatos de intercambio de datos biométricos - Parte 7: Firma / firma de datos de series de tiempo; ISO / IEC 29109-7: 2011 Metodología de prueba de conformidad para formatos de intercambio de datos biométricos definidos en ISO / IEC 19794 - Parte 7: Firma / firma de datos de series de tiempo; ISO / IEC 29109-1: 2009 Metodología de prueba de conformidad generalizada. Como en el caso de la firma electrónica, hay numerosas aplicaciones gratuitas y de libre uso que permiten implementar el método

propuesto en esta invención.

Se ha realizado un amplio estudio sobre las patentes existentes y ninguna de ellas describe los métodos reivindicados en esta invención, ni resuelve las debilidades descritas anteriormente. Concretamente:

Dispositivo, sistema y método para el registro y la autentificación de firmas manuscritas y archivar información manuscrita, patente número de publicación ES2554686 T3. Describe un procedimiento por el cual empleando una pluma electrónica, realiza firmas manuscritas que quedan registradas en un servidor remoto, con el fin de autenticar usuarios previamente registrados.

Procedimiento de autentificación electrónica de una firma manuscrita, módulo y programa informático correspondientes, patente número de publicación ES2531240 T3. Describe el procedimiento de capturar una firma realizada de forma local, con el fin de autenticar la propia firma.

Procedimiento propuesto por la patente número de publicación ES2377787 A1 "Método de firma electrónica garantizada", que describe un procedimiento en el que un servidor remoto se encarga de garantizar el proceso de firma realizado localmente por un firmante.

La publicación "Moderne Verfahren der Kryptographie" ("Procedimientos modernos de criptografía") Beutelspacher, Schwenk, Wolfenstetter, 3. Edición, 1999, Vieweg Verlag, contiene una descripción detallada de los procedimientos criptográficos de clave pública.

El sistema criptográfico RSA que se describe en la Patente de EE.UU. Nº 4.405.829 concedida a Rivest y otros describe un ejemplo de metodología de un sistema criptográfico de clave pública.

La solicitud de patente europea "Method and system for implementing a digital signature" (EP1142194 A1) describe un método para realizar la firma digital en una estación móvil, pero no dice nada sobre el problema de la no repudiación.

La solicitud de patente ‘Electronic document processing system and method of forming digital signature’ (US 5465299 A) describe un método para crear ‘versiones’ de un documento firmado digitalmente, en el que cada versión sucesiva se firma e incluye la firma de la versión anterior.

La patente ‘Method and apparatus for an adapted digital signature’ (US 6615348 B1) describe un algoritmo para generar identidades de usuario usando un algoritmo de firma digital modificado.

La patente ‘Method and apparatus for validating a digital signature’ (US 7178029 B2) describe una forma de verificar que una firma que incluye un certificado digital es válida incluso si el certificado digital ha sido revocado. Es básicamente un servicio de sello de tiempo.

EXPLICACIÓN DE LA INVENCIÓN

La presente invención resuelve los problemas mencionados anteriormente al contemplar la intervención, en el mismo acto en el que el firmante realiza su firma autógrafa, de un segundo usuario que dispone de un certificado de firma electrónica y de un dispositivo de creación de firma que lo emplea para autenticar la firma manuscrita electrónica, también denominada como firma dinámica. Su intervención se basa en aplicar su firma electrónica de criptografía de clave pública, sobre el hash obtenido del conjunto de valores que representan la firma manuscrita electrónica y el documento electrónico.

Con el fin de alcanzar los objetivos y evitar los inconvenientes mencionados en los apartados anteriores, esta invención desarrolla el siguiente procedimiento:

1. En el mercado existen pizarras digitales que tienen la suficiente capacidad de computación y de memoria para desarrollar por si solas y sin conexión a terminal de computación alguna, el método descrito en esta invención. No obstante, también existen pizarras digitales que su capacidad se limita a recoger la firma autógrafa que el firmante realiza sobre su superficie y transmitirla a un terminal informático que se encarga de desarrollar todo el proceso que no es capaz de asumir la pizarra electrónica. En nada afecta uno u otro sistema al método

descrito en esta invención, siendo aplicable a cualquiera de esas opciones: pizarra autónoma o pizarra conectada a un terminal informático. La pizarra digital o el terminal informático al que puede estar conectada, muestra al usuario firmante un documento electrónico que está contenido en su memoria, o que está almacenado en un dispositivo acoplado como por ejemplo un pendrive, o almacenado en un servidor remoto que se consulta con el correspondiente protocolo de comunicaciones, en cualquiera de estas opciones, el objetivo esencial es que el usuario firmante tiene la posibilidad de consultar el documento para el que se le solicita su aceptación.

2. Como expresión de su voluntad de aceptar lo consignado en el documento, realiza una firma autógrafa empleando un puntero o bolígrafo táctil, el cual es aplicado sobre la superficie de una pantalla digital para realizar sobre ella la firma autógrafa, también tiene la posibilidad de incluir un texto manuscrito para realizar un “considerando”, una “salvedad”, o una “mención” o cualquier otra manifestación, incluso reseñar su propia identidad como nombre y cédula de identidad, esta información queda recogida en la imagen de la firma y/o en el grafo. Un software de tratamiento de firma dinámica instalado en la pizarra digital o en el terminal informático es el encargado de capturar el grafo y/o la imagen digital resultante de ese trazado. Se entiende por grafo el conjunto de valores que conforman el patrón biométrico del firmante, habitualmente los parámetros que puede capturar este software, según sensibilidad de la pantalla digital, son: la presión, el ángulo de escritura, la velocidad, la aceleración, la formación de las letras, la forma de los trazos iniciales y finales, la posición y forma de las tildes, los puntos y signos de puntuación, tiempo posición, velocidad, aceleración y la dirección de los rasgos de la firma. Dado que en algunos países se considera información sensible, la aplicación informática puede configurarse para capturar o no el grafo, o incluso cifrarlo sin que ello afecte al método de esta invención. La imagen de la firma digital y/o el grafo quedan recogidos en un archivo informático.

3. Una aplicación informática y un criptosistema instalados en la pizarra digital o en el terminal informático, genera la huella digital (hash) del documento y del grafo y/o la imagen digital resultante de la firma autógrafa del firmante. Para obtener el hash de los archivos. Existen numerosos criptosistemas de código fuente abierto y ampliamente documentados capaces de realizar la elaboración del hash, en la realización preferente de esta invención se utiliza uno de los más

conocidos Bouncy Castle, también existen múltiples algoritmos de digestión públicos que permiten obtener hash seguros, todos ellos ampliamente documentados, siendo el más usual SHA2, empleado en la realización preferente de esta invención. La aplicación que incluye toda la lógica informática para facilitar a los usuarios una interface y llamadas necesarias al criptosistema, es un software extremadamente simple de desarrollo, existen numerosos proyectos de código fuente abierto en Internet que realizar todo este proceso, en la realización preferente se ha desarrollado utilizando el lenguaje de programación Java.

4. El segundo usuario mediante la pizarra digital o el terminal informático, utiliza una el interface de la aplicación informática para seleccionar su certificado de firma electrónica, el cual puede estar almacenado en la pizarra digital, o en el terminal informático, o en un token conectado a la propia tableta digital, o incluso puede estar almacenado en un Servidor de Certificados de Firma Electrónica Remota. Una vez seleccionado el certificado, valiéndose de un teclado informático, o un teclado virtual caso de utilizar la pizarra digital, introduce el PIN de elaboración de firma. La aplicación informática y el criptosistema cuentan con la lógica informática necesaria para intervenir como dispositivo de creación de firma, procediendo a autenticar el hash mediante la creación de una firma electrónica. También se contempla la posibilidad de que previamente este usuario, titular del certificado de firma electrónica, mediante el teclado informático o el teclado virtual, puede haber introducido un texto manuscrito para realizar un “considerando”, una “salvedad”, o una “mención” o cualquier otra manifestación, este texto quedará recogido en un acta que podrá incluir o no también un texto predefinido; en caso de incluir un acta, el algoritmo de hash incluirá esta acta. La inclusión o no de esta acta en nada afecta al método descrito en esta invención. El software necesario para que la aplicación informática y el criptosistema sean dispositivo de creación de firma, es una tecnología muy elemental, con código fuente abierto en internet y ampliamente documentada, no se requieren conocimientos expertos y es accesible a un programador inexperto, al igual que el desarrollo de un teclado virtual y la interface necesaria para que el usuario pueda escribir lo que desee. La generación del acta tampoco requiere especificación relevante alguna, puede quedar recogida en un simple archivo txt, o xml, o pdf, o doc, ennada afecta al objetivo perseguido.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, se acompaña como parte integrante de dicha descripción un juego de dibujos, en los que se ha representado lo siguiente:

Figura 1 ilustra un esquema de captura de grafo (17) y firma digital (18) de una firma autógrafa (13), mostrando los componentes que intervienen: la pizarra digital (1), bolígrafo táctil (12), el programa informático (5) que captura los valores de la firma autógrafa (13), la aplicación informática (6) que muestra el documento electrónico (3) al usuario firmante (11).

Figura 2 ilustra un esquema de generación de un hash (19) del documento (3), de los datos capturados (17) y (18) de la firma autógrafa (13), y elaboración de la firma electrónica (16) que autentica el hash (19) empleando un certificado de firma electrónica (4). Se muestran los componentes que intervienen: la pizarra digital (1), el criptosistema (7) que es invocado por el programa informático (6) para generar el hash (19), el usuario firmante (15) que dispone de un certificado de firma electrónica (4) y utiliza el teclado virtual (27) para introducir el PIN (14) que elabora la firma electrónica (16) autenticando el hash (19).

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

Una realización preferente del sistema aquí descrito, comprende esencialmente, los siguientes elementos:

a) Una pizarra digital (1), con capacidad de computación (procesador y memoria RAM) para lo cual se ha elegido una tablet Surface Pro de Microsoft con un procesador Intel Core i5, que dispone de una video cámara integrada (20), ensambla además un dispositivo de posicionamiento GPS (22), y conexión a internet con el protocolo NTP v.3 conforme al estándar RFC 1305, configurada para obtener la hora (25) con una fuente segura de tiempo hora.roa.es (24), acceso a una Unidad de Sellado de Tiempo de ANF TSA CA tsu1.anf.es para obtener un TimeStamp (26), memoria RAM de 8GB, memoria ROM no volátil (2)

de 256GB SSD, que contiene: un documento electrónico (3), un store en formato PKCS#15 que almacena un certificado de firma electrónica X-509 v.3 (4) con su par de clave privada; un programa informático (5) con capacidad de capturar el grafo (17) y/o imagen digital (18) de la firma autógrafa (13); una aplicación informática (6) que incorpora: un interface de usuario que permite mostrar el documento al usuario firmante (11), un espacio reservado en pantalla para elaborar la firma autógrafa (13) mediante un bolígrafo táctil (12), un procedimiento que permite seleccionar el certificado de firma electrónica (4) e introducir el PIN (14) de generación de firma electrónica mediante un teclado virtual (27), la lógica informática necesaria para interoperar con un criptosistema (7) para elaborar hash (19) e intervenir como dispositivo de creación de firma (29); un criptosistema (7) basado en la librería criptográfica Bouncy Castle, la cual ofrece una amplia colección de API's que contienen los principales algoritmos para procesos criptográficos simétricos AES (8) para cifrado simétrico y algoritmo asimétrico RSA (9) para elaboración de firma electrónica, y que dispone de un algoritmo de digestión para elaboración de hash SHA2 (10). La pizarra digital (1) seleccionada tiene capacidad suficiente para instalar y ejecutar toda la lógica informática, pero podría haberse elegido una pizarra que no tuviera esa capacidad, pero que conectada a una terminal informático (28) como un ordenador personal, el sistema sería igualmente eficaz, sin que ello afecte al método descrito en esta patente, incluso podría ocurrir que el programa informático (6) no contuviera casilla alguna para elaborar sobre ella la firma autógrafa, y que el usuario firmante (11) firmará directamente sobre toda la superficie de la pizarra digital (1), o que se empleara un fichero pdf inteligente capaz de incluir directamente sobre una de sus capas las marcas o textos transcritos por cualquiera de los dos usuarios que intervienen en la transacción: firmante y testigo. Ninguno de los supuestos afecta al método descrito en esta invención.

b) Un usuario firmante (11) en posesión de un bolígrafo táctil (12).

c) Un usuario testigo (15) en posesión del certificado de firma electrónica (4) del cual es titular, y con el conocimiento del PIN (14) de activación de firma que permite elaborar la firma electrónica (16).

d) El programa informático (5). Se ha desarrollado utilizando la API de firma de StepOver https://www.stepoverinfo.net/ . Se trata de una interfaz de programación concebida para usarse con cualquier aplicación individual para la firma electrónica de documentos PDF y PDF/A. La API de firmas introduce el grafo (17) y la imagen

de la firma (18) capturada electrónicamente, además de la firma digital (16) en el documento firmado. Mediante esta API de firmas se puede crear el programa informático. Además de esta API existen otras API similares ampliamente documentadas, incluso programas ya elaborados de carácter gratuito.

e) El programa informático (6) que incorpora interface de usuario, se ha desarrollado una aplicación en Java. Este software tiene toda la lógica requerida y la capacidad de interoperar con el criptosistema (7)

Se realiza el siguiente procedimiento:

1. El documento electrónico (3) se muestra al usuario firmante (11) a través de la pantalla de la Tablet (1) para que pueda revisarlo.
2. El usuario firmante (11), utilizando el bolígrafo táctil (12) realiza la firma autógrafa (13) sobre la Tablet (1).
3. El programa informático (5) procede a la captura del grafo (17) y de la imagen de la firma (18).
4. El usuario testigo (15) empleando la Tablet (1), y utilizando el Interface del programa informático (6), selecciona el certificado de firma electrónica (4) e introduce mediante el teclado virtual (27) su PIN (14).
5. El programa informático (6) utilizando el criptosistema (7) genera un hash (19) del documento electrónico (3), del grafo (17), y de la imagen de la firma manuscrita electrónica (18).
6. El criptosistema (7) firma electrónicamente el hash (19) obteniendo una firma electrónica (16). De esta forma todos los archivos quedan asociados y su integridad está garantizada. En esta configuración no se ha permitido que el usuario testigo seleccione archivo de documento electrónico o valores de la firma manuscrita electrónica de los que se obtiene el hash (19). Esta automatización se ha realizado como medida de seguridad para impedir el error humano, fortuito o intencionado, pero nada impide incluir esta selección sin que ello afecte al método escrito en esta invención. Este método contempla la posibilidad de que el certificado de firma electrónica (4) este almacenado en un Servidor Remoto de Certificados Centralizados tal y como lo permite el Reglamento (UE) 910/2014 eIDAS, en cuyo caso el criptosistema que interviene como dispositivo de creación de firma está en ese servidor remoto y, por lo tanto, el hash (19) se envía por canal seguro SSL o TLS a ese servidor para ser firmado, de acuerdo con el Reglamento eIDAS es el

prestador cualificado de servicios de confianza que administra este servidor remoto, el que dota al sistema de los procedimientos técnicos necesarios para comunicar PIN y hash, así como para recibir la firma electrónica resultante. Nada impide incluir el uso de este servidor remoto sin que ello afecte al método descrito en esta invención.

El hash (19) es obtenido por el criptosistema (7) mediante la correspondiente llamada al algoritmo de digestión SHA2, el cual es aplicado como se indicaba anteriormente sobre los archivos documento electrónico (3), grafo (17) y firma digital (18). No obstante, si el usuario testigo (15) ha introducido un texto con considerando, mención, salvedad, o texto predefinido incluido en un acta, el hash (19) incluirá este acta. Nada impide incluir esta información sin que ello afecte al método descrito en esta invención.

Los estándares ETSI, ISO y RFC mencionados más arriba incluyen descripciones técnicas muy pormenorizadas.

Además del procedimiento descrito en esta realización preferente, esta patente incluye diversas reivindicaciones cuyos procesos, aunque muy simples de realización, presuponen importantes mejoras sobre la reivindicación principal.

La reivindicación 2. Prácticamente todas las Tablet (1) del mercado incorporan una cámara de video (20) y hay numerosas APIs de código fuente abierto que permiten ordenar al sistema operativo de la pizarra digital (1) realizar una fotografía o incluso, realizar una grabación de video. El formato de la adquisición siempre es configurable, aunque habitualmente se utiliza formato JPEG para un archivo de imagen, o MP4 para un archivo de video. El algoritmo de digestión se puede utilizar en cualquier formato de fichero, no tiene limitación alguna al respecto. Toda la tecnología necesaria para desarrollar la reivindicación 2, está disponible públicamente y ampliamente documentada, es accesible para cualquier programador por inexperto que sea. Existen otras modalidades de realizar la programación de la lógica informática, ninguna afecta al procedimiento ni a la reivindicación.

La reivindicación 3. Prácticamente todas las Tablet (1) del mercado incorporan una dispositivo de posicionamiento GPS (20) que permite determinar la geoposición de la Tablet en cada momento. Hay numerosas APIs de código fuente abierto que permiten ordenar al sistema operativo de la pizarra digital (1) realizar una lectura de la

geoposición en que se encuentra. El formato de la adquisición siempre es configurable, aunque habitualmente se utiliza un simple archivo TXT. El algoritmo de digestión se puede utilizar en cualquier formato de fichero, no tiene limitación alguna al respecto. Toda la tecnología necesaria para desarrollar la reivindicación 3, está disponible públicamente y ampliamente documentada, es accesible para cualquier programador por inexperto que sea. Existen otras modalidades de realizar la programación de la lógica informática, ninguna afecta al procedimiento ni a la reivindicación.

La reivindicación 4. Prácticamente todas las Tablet (1) del mercado incorporan conectividad a Internet. Existen numerosas fuentes seguras de tiempo que son de libre y gratuito acceso. En España la fuente de tiempo más utilizada en la del Laboratorio del Real Observatorio de la Armada (ROA) que permite determinar con una exactitud de segundo el tiempo UTC actual (en inglés, Coordinated Universal Time). Para la consulta de tiempo se emplea el protocolo publico NTP, existen numerosas APIs de código fuente abierto que permiten realizar estas consultas. La información puede quedar registrada en un simple archivo TXT. El algoritmo de digestión se puede utilizar en cualquier formato de fichero, no tiene limitación alguna al respecto. Toda la tecnología necesaria para desarrollar la reivindicación 3, está disponible públicamente y ampliamente documentada, es accesible para cualquier programador por inexperto que sea. Existen otras modalidades de realizar la programación de la lógica informática, ninguna afecta al procedimiento ni a la reivindicación.

La reivindicación 6. La inclusión de varios firmantes en un proceso de firma secuencial requiere una lógica informática elemental, tan simple que un programador de informática inexperto puede elaborarla. Básicamente solo se precisa incluir un dos botones “continuar proceso” “cerrar proceso”. Al pulsar “continuar proceso” simplemente genera el archivo de la firma manuscrita electrónica y abre la posibilidad de realizar una nueva firma; al pulsar “cerrar proceso” simplemente genera el archivo de la firma manuscrita electrónica, y da por finalizada la captura de firmas y continua el paso siguiente. Existen otras modalidades de realizar la programación de la lógica informática, ninguna afecta al procedimiento ni a la reivindicación.

La reivindicación 7. La captura del momento del tiempo ya ha quedado explicada en la reivindicación 4, esta reivindicación solo requiere una lógica informática elemental, tan simple como realizar un cálculo del tiempo transcurrido entre el momento que firmó el

usuario (11) y el momento en que desea firmar el usuario (15), si el tiempo transcurrido es superior a un tiempo de referencia que consta registrado en una archivo de recursos al que tiene acceso la aplicación informática (6) y que puede ser configurado por el fabricante o por el propio usuario de la aplicación, se impide que el usuario (15) firme. Es decir el programador solo tiene que realizar una simple comparación y calcular si el tiempo transcurrido es menor, igual o mayor, si es mayor, parar el proceso. Existen otras modalidades de realizar la programación de la lógica informática, ninguna afecta al procedimiento ni a la reivindicación.

REIVINDICACIONES

1.- Método para autenticar una firma dinámica con el documento firmado mediante una firma electrónica, que comprende:

Paso 1: Se dispone de una pizarra digital (1), que conectada a un terminal informático (28) o de forma autónoma, dispone de un programa informático (6) que permite visualizar un documento electrónico (3) contenido en la pizarra digital (1) o en el terminal informático (28),

Paso 2: El usuario firmante (11) dispone de un bolígrafo táctil (12), y un programa informático (6) que permite que el usuario firmante (11) elabore una firma autógrafa (13) sobre la superficie de la pizarra digital (1).

Paso 3. El programa informático (5) realiza una captura del grafo (17) y/o imagen de firma digitalizada (18).

Paso 4: La pizarra digital (1) o el terminal informático al que se conecta (28) incluye el programa informático (6) que incluye la lógica informática necesaria para utilizar un criptosistema (7) que genera un hash (19) del documento electrónico (3) y los archivos grafo (17) e imagen de firma digitalizada (18).

Paso 5: Caracterizado porque en el acto de firma descrito anteriormente, interviene un segundo usuario (15) que dispone de un certificado de firma electrónica (4), y que emplea un programa informático (6) instalado en la pizarra digital (1) o terminal informático (28), que le permite introducir el PIN (14) y que tiene la capacidad de activar un proceso de firma sobre el hash (19), obteniendo una firma electrónica (16), que autentica ese hash (19), quedando así asociados de forma indisoluble todos los archivos y garantizando la integridad de los mismos.

2.- Procedimiento según Reivindicación 1, caracterizado porque en el Paso 2 y Paso 4 comprenden además:

Paso 2: La pizarra digital (1), incluye una cámara de video (20), y el programa informático (6) incluye la lógica necesaria para que en el momento de elaborar la firma autógrafa

(13), se capture la imagen del usuario (21) firmante en el momento de realizar la firma.
Paso 4: El programa informático (6) dispone de la lógica informática necesaria para incluir el archivo de la imagen del usuario (21) en el proceso de obtención del hash (19), de tal forma que la imagen (21) queda asociada al resto de archivos.

3.- Procedimiento según Reivindicación 1, caracterizado porque en el Paso 2 y Paso 4 comprenden además:

Paso 2: La pizarra digital (1), incluye un sistema de geo-posicionamiento GPS (22), y el programa informático (6) incluye la lógica necesaria para que en el momento de elaborar la firma autógrafa (13) se proceda a capturar la posición geográfica (23) del firmante en el momento de realizar la firma.
Paso 4: El programa informático (6) dispone de la lógica informática necesaria para incluir el archivo de geoposición (23) en el proceso de obtención del hash (19), de tal forma que la posición geográfica (23) queda asociada al resto de archivos.

4.- Procedimiento según Reivindicación 1, caracterizado porque en el Paso 2 y Paso 4 comprenden además:

Paso 2: El programa informático (6), incluye un protocolo de comunicación con una fuente segura de tiempo (24), y el programa informático (6) incluye la lógica necesaria para que en el momento de elaborar la firma autógrafa (13) se proceda a capturar el momento en el tiempo (25) en que se está realizando la firma.
Paso 4: El programa informático (6) dispone de la lógica informática necesaria para incluir el archivo de momento en el tiempo (25) en el proceso de obtención del hash (19), de tal forma que el momento en el tiempo (25) queda asociado al resto de archivos.

5.- Procedimiento según Reivindicación 1, caracterizado porque en el Paso 4 y Paso 5 comprenden además:

Paso 4: El programa informático (6), incluye un protocolo de comunicación con un servidor de sellado de tiempo electrónico (26), y la lógica informática necesaria para enviar al servidor de sellado de tiempo el hash (19) y recibir un sello de tiempo electrónico (26) que está asociado indisolublemente a ese hash (19)
Paso 5: El programa informático (6), incluye un protocolo de comunicación con un

servidor de sellado de tiempo electrónico (26), y la lógica informática necesaria para que la firma electrónica (16) incluya sello de tiempo.

6.- Procedimiento según Reivindicación 1, caracterizado porque en el Paso 2, Paso 3, y Paso 4 comprenden además:

Paso 2: El programa informático (6) dispone de la lógica informática necesaria para permitir la intervención de varios firmantes (11), el proceso se basa en la elaboración de firmas secuencialmente, hasta que el último firmante indica que es la última firma autógrafa.

Paso 3: El programa informático (5) realiza una captura del grafo (17) y/o imagen de firma digitalizada (18) de cada usuario firmante (11) generando un archivo independiente de cada intervención.

Paso 4: El programa informático (6), incluye la lógica informática necesaria para generar el hash (19) incluyendo todos los archivos de firma de cada uno de los usuarios firmantes (11)

7.- Procedimiento según Reivindicación 1, caracterizado porque en el Paso 2 y Paso 5 comprende además:

Paso 2: El programa informático (6), incluye un protocolo de comunicación con una fuente segura de tiempo (24), y el programa informático (6) incluye la lógica necesaria para que en el momento de elaborar la firma autógrafa (13) se proceda a capturar el momento en el tiempo (25) en que el usuario firmante (11) se está realizando la firma, esta información queda almacenada en una posición de memoria del programa informático (6).

Paso 5: El programa informático (6) dispone de la lógica informática necesaria para que antes de que el segundo usuario firmante (15) elabore su firma, realice una consulta a la fuente segura de tiempo para determinar el intervalo de tiempo transcurrido entre que firmó el usuario firmante (11) y el momento actual. La lógica incorpora un rango de tiempo de seguridad que determina que sobre pasado el tiempo de seguridad, se impida firmar al segundo usuario firmante (15).

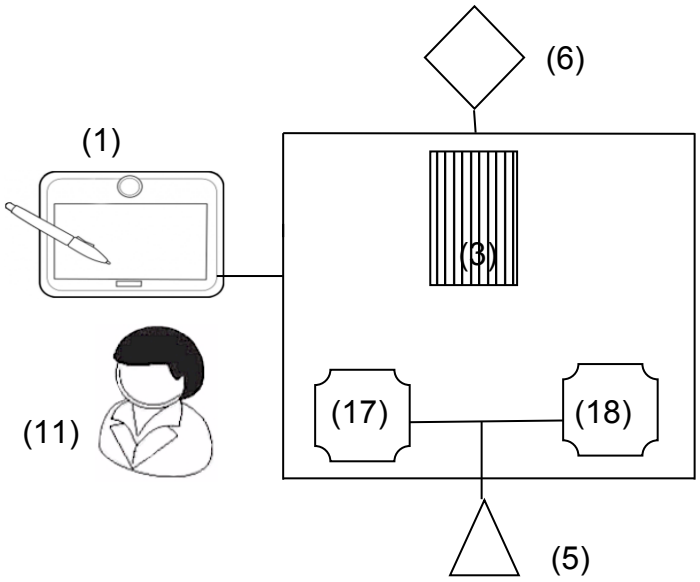

Figura 1

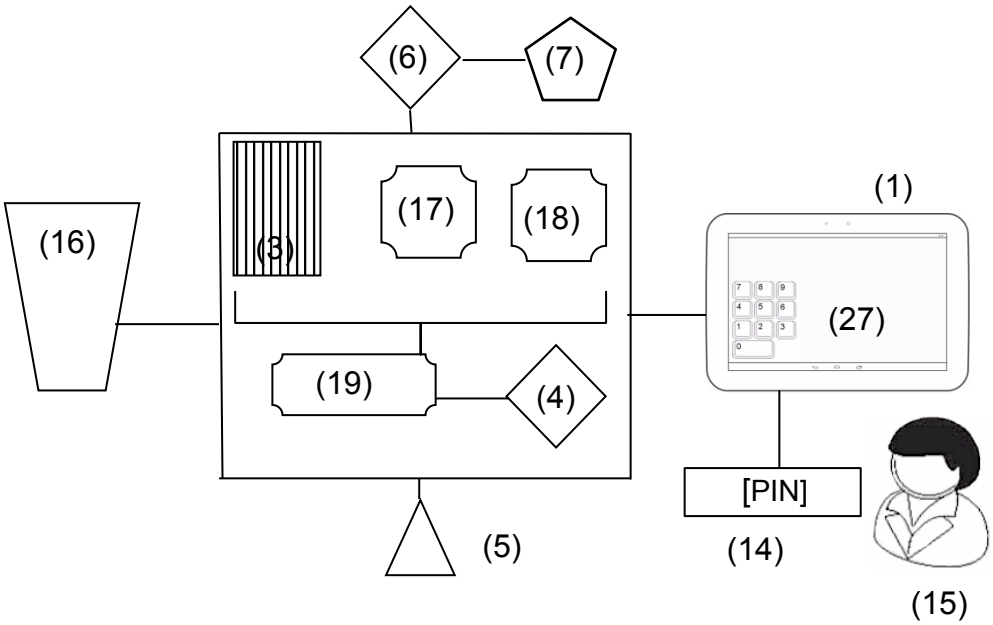

Figura 2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201731397

(22) Fecha de presentación de la solicitud: 11.12.2017

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/00*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	CA 2511780 A1 (MORIN JEAN-GREGOIRE et al.) 11/01/2007, Resumen Epodoc	1-7
A	US 2002128969 A1 (PARMELEE CHRISTOPHER L et al.) 12/09/2002, Todo el documento.	1-7
A	US 2005201561 A1 (KOMANO YUICHI et al.) 15/09/2005, Todo el documento.	1-7
A	KR 101789298B B1 (FINOTEK) 20/11/2017, Todo el documento.	1-7
A	EP 2328018 A1 (CRAMBO SA et al.) 01/06/2011, Todo el documento.	1-7
A	US 2016337806 A1 (SCHURR RONALD C et al.) 17/11/2016, Todo el documento.	1-7
A	US 2008148054 A1 (CAHILL JASON et al.) 19/06/2008, Todo el documento.	1-7

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
05.12.2018	M. Muñoz Sanchez	1/2

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI