

	Espacio reservado para el adhesivo de radicación
---	--

DIRECCIÓN DE NUEVAS CREACIONES
PROCEDIMIENTO ACCELERADO DE EXÁMENES DE PATENTE (PPH)

1	NÚMERO DE SOLICITUD ANTE LA SIC	NC2022/0000102	
2	OFICINA DE PRIMERA PRESENTACIÓN (OPP)	MÉXICO	
3	NÚMERO(S) DE SOLICITUD O PUBLICACIÓN DE LA(S) SOLICITUD(ES) (OPP):	1. MX/a/2019/008404 2. WO/2021/010811 3.	
4	☐ REPRESENTANTE LEGAL ☒ APODERADO		
APELLIDOS DELGADO VILLEGAS		NOMBRES CLEMENCIA	IDENTIFICACIÓN C.C. 51.663.741 T.P. 43.307
DIRECCIÓN Avda. Carrera 24 No, 37 – 31 Of. 202 CIUDAD BOGOTA D.C. PAÍS COLOMBIA		No. TELÉFONO 6012444096 CORREO ELECTRÓNICO mde@mdelaw.com No. RADICACIÓN O PROTOCOLO DE PODER GENERAL	
5	CONDICIONES PARA ACCEDER A ESTE PROCESO:		
5.1. DATOS DE PRIORIDAD ☒ SI ☐ NO			
(33) PAÍS DE ORIGEN 1. MÉXICO 2. 3.		CÓDIGO PAÍS MX	(31) NÚMERO MX/a/2019/008404 (32) FECHA (AAAA/MM/DD) 2019/07/12
5.2. DATOS SOLICITUD INTERNACIONAL PCT ☒ SI ☐ NO			
Solicitud Internacional No. PCT/ MX2020/05009		Fecha 2020/06/09	
Publicación Internacional No. WO /2021/010811A1		Fecha 2021/01/21	
El solicitante presenta una copia de la(s) reivindicación(es) patentable(s) u otorgable(s) de la solicitud de la Oficina de Primera Presentación que profirió el examen de patentabilidad, junto con una traducción al castellano. ☒ SI ☐ NO			
REQUISITOS PARA EL RECONOCIMIENTO DE LOS RESULTADOS DE EXÁMENES DE PATENTABILIDAD EFECTUADOS A SOLICITUDES EXTRANJERAS			
Para que la Superintendencia de Industria y Comercio pueda reconocer los resultados de exámenes de patentabilidad producidos por otras Oficinas de Propiedad Industrial se debe cumplir con las siguientes condiciones:			
(a) Al momento de solicitar el examen de patentabilidad, si el solicitante pide que se reconozcan exámenes de patentabilidad de otras oficinas extranjeras, deberá aportar junto con el pago de la tasa correspondiente, los siguientes anexos:			
(i) Copia de las resoluciones, fallos o decisiones que han sido relevantes para la determinación de la patentabilidad de la(s) solicitud(es) en la Oficina que haya proferido el examen de patentabilidad que contienen reivindicaciones patentables u otorgables que son la base de la petición, y si es del caso, su traducción al castellano. ☒ SI ☐ NO			
(ii) Copia de todas las reivindicaciones determinadas como patentables u otorgables en la Oficina que profirió el examen de patentabilidad y, si es del caso, su traducción al castellano. ☒ SI ☐ NO			
(iii) Copia de los antecedentes, información o documentos citados por el examinador de la Oficina de Primera Presentación del examen de patentabilidad, en las resoluciones, fallos o decisiones correspondientes, incluyendo la literatura no patente. Los documentos de patente deberán presentarse siempre y cuando no estén disponibles para la Superintendencia de Industria y Comercio mediante el simple acceso a bases de datos gratuitas. ☐ SI ☒ NO			
(iv) Una tabla de correspondencias de las reivindicaciones que han sido determinadas como patentables u otorgables en la solicitud de la Oficina que haya proferido el examen de patentabilidad.			
7	FIRMA DEL SOLICITANTE, DEL APODERADO O DEL REPRESENTANTE LEGAL <i> Junto a cada firma, indicar el nombre del firmante y su calidad (si tal calidad no es obvia al leer el petitorio)</i>		
Clemencia Delgado V. CLEMENCIA DELGADO VILLEGAS INDUSTRIA Y COMERCIO			

6	TABLA DE CORRESPONDENCIA DE REIVINDICACIONES		
Reivindicaciones en la solicitud en Colombia		Reivindicaciones otorgables en la solicitud internacional	Explicación sobre la suficiente correspondencia ó Comentarios que explican la correspondencia
Reivindicaciones 1 a 9 que corresponden a las reivindicaciones originales presentadas en el PCT 1-9		Reivindicaciones 1 a 9 concedidas por el Instituto Mexicano de la Propiedad Industrial bajo el No.384943 del 29 de julio de 2021, ver Anexo. 1-9	Las Reivindicaciones de la solicitud en Colombia son las mismas que las Reivindicaciones Concedidas en México SON LO MISMO



TÍTULO DE PATENTE No. 384943

Titular(es): MUUK TECHNOLOGIES, S. DE R.L. DE C.V.

Domicilio: Fuente de Pirámides 1, No. 604, Lomas de Tecamachalco, Naucalpan de Juárez, Estado de México, 53950, MÉXICO

Denominación: SISTEMA PARA GENERAR FIRMA AUTÓGRAFA DIGITAL POR MEDIO DE UN DISPOSITIVO MÓVIL.

Clasificación: **CIP:** G06F21/64; G06F21/30; G06F21/33; G06F21/45; G06Q20/12; H04L9/32
CPC: G06F21/64; G06F21/30; G06F21/33; G06F21/45; G06Q20/12; H04L9/32

Inventor(es): CARLOS EDUARDO CHAVARRIA GUTIERREZ

SOLICITUD

Número:
MX/a/2019/008404

Fecha de Presentación:
12 de Julio de 2019

Hora:
14:37

Vigencia: Veinte años

Fecha de Vencimiento: 12 de julio de 2039

Fecha de Expedición: 29 de julio de 2021

La patente de referencia se otorga con fundamento en los artículos 1º, 2º fracción V, 6º fracción III, y 59 de la Ley de la Propiedad Industrial.

De conformidad con el artículo 23 de la Ley de la Propiedad Industrial, la presente patente tiene una vigencia de veinte años improrrogables, contada a partir de la fecha de presentación de la solicitud y estará sujeta al pago de la tarifa para mantener vigentes los derechos.

Quien suscribe el presente título lo hace con fundamento en lo dispuesto por los artículos 5º fracción I, 9, 10 y 119 de la Ley Federal de Protección a la Propiedad Industrial; artículos 1º, 3º fracción V, inciso a), 4º y 12º fracciones I y III del Reglamento del Instituto Mexicano de la Propiedad Industrial; artículos 1º, 3º, 4º, 5º fracción V, inciso a), 16 fracciones I y III y 30 del Estatuto Orgánico del Instituto Mexicano de la Propiedad Industrial; 1º, 3º y 5º fracción I Acuerdo Delegatorio de Facultades del Instituto Mexicano de la Propiedad Industrial.

El presente documento electrónico ha sido firmado mediante el uso de la firma electrónica avanzada por el servidor público competente, amparada por un certificado digital vigente a la fecha de su elaboración, y es válido de conformidad con lo dispuesto en los artículos 7 y 9 fracción I de la Ley de Firma Electrónica Avanzada y artículo 12 de su Reglamento. Su integridad y autoría, se podrá comprobar en www.gob.mx/impj.

Asimismo, se emitió conforme lo previsto por los artículos 1º fracción III; 2º fracción VI; 37, 38 y 39 del Acuerdo por el que se establecen lineamientos en materia de Servicios Electrónicos del Instituto Mexicano de la Propiedad Industrial.

SUBDIRECTOR DIVISIONAL DE EXAMEN DE FONDO DE PATENTES ÁREAS MECÁNICA, ELÉCTRICA Y DE DISEÑOS INDUSTRIALES Y MODELOS DE UTILIDAD

PEDRO DAVID FRAGOSO LÓPEZ



Cadena Original:
PEDRO DAVID FRAGOSO LOPEZ|00001000000506606281|SERVICIO DE ADMINISTRACION
TRIBUTARIA|1052||MX/2021/75639|MX/a/2019/008404|Título de patente normal|1027|RGZ|Pág(s)
1|59A24NfHcVMI5YYfMTAv+aHZ7rI=

Sello Digital:
C4IPd+tiDPOYnL9N+TVboaoWCiFOkxABD0ktYFTKq/oxSGjWIDSQkh4gukSqmS6G6mFoHegSgEfQAJjs1AD4Ban0KA
YoYamLMgYTswncAE2atIvMXQARvydvwDQIP68xo4YAavBNJJu/KBGvho9hGrmOV6rX20z5SbhxGMxg9/0vKO6TchbF
I6x8FatExQ5B12svU74aLf0yO9JgGbWzDpIQAQWwhsQq3Si0v0jb0pcBZjSiSgjQr+aPHR7ax968NpINgaZK7ZNAxy
m7mXksWQZchMD3ejfWZq0D23qxvdPv0upISQWF9hG7a/m/CTYSm7rkITaKqSHTSxar7XHNA==



MX/2021/75639

SISTEMA PARA GENERAR FIRMA AUTÓGRAFA DIGITAL POR MEDIO DE UN DISPOSITIVO MÓVIL

5

CAMPO TÉCNICO

La presente invención pertenece al campo técnico de las comunicaciones, específicamente al campo de la comunicación de dispositivos móviles en conjunto con los sistemas de cómputo y la seguridad de documentos, y de forma más específica con la firma de documentos de forma digital y la seguridad en la comunicación para garantizar la integridad del documento.

ANTECEDENTES

En la actualidad, el desarrollo del comercio electrónico y el intercambio de bienes entre los diferentes sectores de la sociedad, hace necesario de realizar convenios o cerrar contratos, que la forma convencional, es firmando documentos en papel, hecho que se ha realizado desde las antiguas culturas y se ha mantenido a lo largo de los años, sin embargo, con la evolución tecnológica, se conocen modalidades de realizar el proceso de firma de documentos, de tal manera que muestra una forma alterna para firmar documentos y así tener ventajas con respecto a la forma tradicional de realizar la firma de un documento.

Tomando en cuenta lo anterior y al observar el estado de la técnica, se ha encontrado el documento de patente US 6 839 453 el cual describe un sistema y método para autenticar una firma en un artículo firmado originalmente, que emplea al menos una cámara para capturar una imagen de una persona cuando se firma el artículo. En una realización, la imagen es una imagen de video en tiempo real, y en otra realización, la imagen es una foto fija. Las imágenes asociadas con el artículo firmado, de modo que el titular del artículo tenga un mecanismo para autenticar la firma. Preferiblemente, el artículo firmado tiene un identificador único ubicado en él, y

la imagen se edita preferiblemente para incluir también ese identificador. También se proporciona un kit de recuerdos, que contiene un artículo firmado originalmente, un medio de almacenamiento que almacena una imagen capturada de un evento de firma original asociado con el artículo. Además, una imagen capturada y los datos indicativos del artículo firmado se almacenan electrónicamente en asociación entre sí, como en un medio de almacenamiento disponible para un titular del artículo firmado, o en una base de datos a la que se puede acceder de forma remota.

Otro documento relacionado es la solicitud de patente US 2013050512 A1, este documento describe las técnicas para la firma de documentos electrónicos iniciada por el firmante a través de un servicio de firma electrónica utilizando un dispositivo móvil u otro dispositivo cliente. Las formas de realización por ejemplo es proporcionar un servicio de firmas electrónicas ("ESS") configurado para facilitar la creación, el almacenamiento y la gestión de documentos y las firmas electrónicas correspondientes. En algunas realizaciones, cuando un usuario firmante recibe una copia impresa (por ejemplo, un documento de firma), el firmante puede capturar una imagen del documento de firma con una cámara de un dispositivo móvil. El firmante puede importar la imagen capturada en el ESS para su firma, almacenamiento y / o transmisión a otras partes.

También la solicitud de patente US 2012284591 A1 describe sistemas y métodos para la identificación y firma electrónica de documentos electrónicos. Ciertas realizaciones de la presente invención proporcionan una herramienta de firma virtual para crear una firma electrónica única y verificable (SigCode) para firmar documentos usando un dispositivo móvil de un individuo. En algunas realizaciones, los identificadores de documentos (por ejemplo, códigos QR) se pueden usar para identificar y recuperar documentos para la firma digital. Por ejemplo, al escanear otro identificador de documento, se puede recuperar de un servidor una versión electrónica del documento (por ejemplo, una exención). El documento electrónico se puede mostrar en el dispositivo móvil del usuario (por ejemplo, a través de una página web). Luego, el usuario puede revisar el documento electrónico, completar la información

requerida y firmar el documento con una firma electrónica generada por la herramienta de firma electrónica.

Otro documento, es la solicitud de patente US 2012093409 A1 que describe sistemas, métodos y medios legibles por computadora para capturar una firma y colocar una representación de la firma capturada en el campo apropiado de un documento. Una cámara u otro sensor apropiado puede capturar una imagen de una firma proporcionada por un usuario en un papel. La firma se puede digitalizar para crear una representación que un dispositivo puede usar en un documento visualizado. Para determinar dónde colocar la representación, se puede identificar una línea horizontal de un documento representando de manera selectiva porciones del documento adyacentes a una posición de entrada, e identificando uno o más límites para una línea horizontal detectada. La representación se puede escalar para ajustarse a un campo detectado del documento.

15

La patente US 8780383 B2, describe un documento de fax que puede cargarse en un servidor de fax en una red vPBX o generarse dinámicamente. Para la generación dinámica, las plantillas preconfiguradas se pueden almacenar en un dispositivo móvil o en un servidor de fax. Un usuario puede usar un dispositivo móvil conectado a una red vPBX como dispositivo de control para dirigir la generación de faxes en un servidor de fax. La generación de faxes se puede personalizar en función de la ubicación geográfica del dispositivo móvil. El fax generado se puede descargar en un dispositivo móvil. El usuario puede firmar digitalmente el fax utilizando un dispositivo de entrada de pantalla táctil en el dispositivo móvil. El fax firmado digitalmente se puede transmitir a un dispositivo de destino.

25

La solicitud de patente US 2005166053 A1 describe un método, aparato y sistema que están dirigidos a asociar la firma de un dispositivo con un dispositivo móvil. La invención está configurada para determinar al menos un nivel de confianza asociado con el dispositivo móvil y una pasarela de portadora asociada. En una realización, el dispositivo móvil puede tener múltiples niveles de confianza asociados

30

con él. Se puede determinar un nivel de confianza en función de si el dispositivo móvil proporciona un identificador de dispositivo. Se puede determinar otro nivel de confianza en función de si el dispositivo móvil está configurado para recibir una cookie. Todavía se puede determinar un tercer nivel de confianza en función de un identificador de sesión dinámico. El nivel de confianza también puede determinarse basándose, en parte, en una confianza asociada con la puerta de enlace del operador.

La patente US 8056822 B2 describe un método para certificar y posteriormente autenticar documentos físicos o digitales originales. El concepto de evidencia se basa en la naturaleza dual de un elemento de información física y un elemento de información digital, uno de los cuales es la referencia para el otro que no puede modificarse con el riesgo de perder la evidencia. Para un documento original físico (8) asociado con un sello de burbuja (7), hay una contraparte de referencia sin papel patentada y con fecha y hora correspondiente. Para un documento digital original patentado, estampado con fecha y hora (15), hay una contraparte de referencia correspondiente en forma de sello de burbuja (7)

La patente US 6839453 B1, la cual describe un método y un sistema para proporcionar a los propietarios, compradores potenciales y otros usuarios de artículos autografiados, como artículos deportivos y otros recuerdos de entretenimiento, evidencia visual para verificar la autenticidad del autógrafo. Un método de la presente invención implica capturar una imagen de la firma cuando se coloca en el artículo. La imagen así capturada se almacena en un medio legible por computadora. Además del artículo en sí, al propietario del artículo se le puede proporcionar un medio legible por computadora que contiene instrucciones legibles por computadora para acceder a la imagen y otra información sobre el artículo, el proceso de firma, el autógrafo, etc. La imagen puede ser capturada por una cámara montada en un bolígrafo u otro instrumento de escritura.

La tecnología que actualmente se encuentra, nos da la posibilidad de modificar la forma tradicional de realizar las firmas autógrafas para cerrar convenios o contratos,

de tal forma que al hacer uso de los dispositivos móviles y las redes de comunicación se realiza la presente invención, la cual supera el problema de poder realizar la firma autógrafa directamente en el dispositivo móvil, de tal forma que se garantiza la integridad del documento firmado.

5

OBJETO DE LA INVENCION

Un objetivo de la presente invención, es proveer un sistema de seguridad que nos permite realizar una firma autógrafa digital, esta nueva firma autógrafa digital evita la suplantación de identidad del firmante, esto por medio de una interfaz que se encuentra en un dispositivo móvil, el cual, cuando un usuario desea realizar una firma autógrafa digital, lo realiza por medio de esta interface, la cual activa la función de la activación de la cámara de video y realiza un video del momento en que se está realizando la firma en el mismo dispositivo móvil, en el cual, por medio de dicha interface, se habilita un campo que es mostrado en la pantalla en donde el usuario pueda trazar su firma, la cual queda incrustada en el video y que al procesar los datos, se genera el documento en PDF en el cual se incorpora la firma del usuario como si realmente hubiera firmado directamente en el papel. Para garantizar la integridad de este proceso, se realizan diferentes etapas o paso con las cuales se mantiene la seguridad de la información.

Otro objetivo, es el de implementar un método, el cual se lleva a cabo por medio de un dispositivo móvil, y que se encarga de activar una interface en el dispositivo móvil para que un usuario pueda realizar una firma autógrafa digital y obtener un documento en PDF con la firma autógrafa. El método activa una interface en el dispositivo móvil para realizar el trazo de la firma en el dispositivo móvil, implementando también las etapas necesarias con las cuales se garantiza la seguridad de la información.

Un objetivo más, es el de un medio legible por computadora el cual contiene los pasos de un método para que un usuario pueda realizar una firma autógrafa digital en

un dispositivo móvil, en donde el método activa una interface en el dispositivo móvil permitiendo al usuario trazar su firma y el dispositivo móvil captura dicha firma mientras toma un video del usuario firmando, para que, al finalizar el proceso, el usuario puede tener el documento firmado en formato PDF. Lo anterior se realiza incorporando etapas
5 o pasos de seguridad para conservar la integridad del proceso.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

La presente invención describe un sistema para generar firmas autógrafas
10 digitales (FAD) por medio de un dispositivo móvil, el sistema consiste de con diferentes componentes que al integrarse, se obtiene un documento con la firma autógrafa, este sistema comprende una interfaz que es incorporada en un dispositivo móvil, y por medio de la interface ya incorporada en el dispositivo móvil, puede obtener el documento que desea firma, este se realiza por medio de un código QR o link que es
15 recibido por medio de un mensaje en el dispositivo móvil.

Una vez que el usuario decido realizar la firma del documento obtenido por le código QR o el link, entonces la interface en el dispositivo móvil muestra un campo en el mismo para que el usuario pueda trazar la firma con el dedo, este mientras que la
20 interface activa la cámara del dispositivo móvil y se observa la imagen del usuario en la pantalla, y así se generan dos videos uno de la imagen del usuario trazando su firma sobre la pantalla del dispositivo móvil, y otro video cuando el usuario realiza una lectura de las condiciones de la firma. Con los videos obtenidos de esta forma, se integra el proceso de seguridad, para lo cual la interface de la firma autógrafa digital encripta y
25 envía los datos a los servidores de las instituciones que forman parte de la comprobación de la seguridad y también de la institución que genera el documento. Adicionalmente, el sistema de la firma autógrafa digital agrega dos mecanismos de seguridad, y envía copias del documento firmado a las partes.

30 También se describe un método en un sistema para generar firmas autógrafas digitales en un dispositivo móvil, por lo que el método consiste en incorporar una

interface en un dispositivo móvil; obtener el documento a firmar mediante un código QR o un link, los cuales son recibidos por medio de un mensaje MSM en el dispositivo móvil, un usuario, por medio del dispositivo móvil, realiza el trazo de su firma sobre la pantalla del dispositivo móvil, para que posteriormente sea procesada la firma. La

5 interface de la firma autógrafa digital, se encarga de encriptar la información, enviarla a los servidores de computo de las instituciones que forman parte de la seguridad del sistema, y como una medida de seguridad, se elimina toda la información que fue procesada en el dispositivo, para finalmente el sistema de la firma autógrafa digital agrega dos mecanismos de seguridad adicionales al archivo y además envía copia del

10 documento firmado a las partes.

Adicionalmente, se describe un medio legible por computadora, que contiene los pasos para poder realizar la incorporación de la interface en un dispositivo móvil, para posteriormente obtener el documento a firmar ya sea por medio de un código QR

15 o un link que se obtienen de un mensaje SMS al dispositivo móvil, para después activar la interface del dispositivo móvil y realizar dos videos del usuario trazando su firma sobre la pantalla del dispositivo móvil y, de la lectura del contenido del documento firmado, por ejemplo, del dispositivo móvil, y con esto, poder mandar por medio del dispositivo móvil y de acuerdo a las indicaciones del sistema de la firma autónoma

20 digital, encripta la información y es enviada a los servidores para su validación y conservación, borrando todo contenido del dispositivo móvil.

BREVE DESCRIPCIÓN DE LAS FIGURAS

25 **Figura 1.** Muestra un diagrama de flujo general del sistema.

Figura 2. Muestra un diagrama de flujo correspondiente a la obtención de la información.

30 **Figura 3.** Muestra una modalidad del diagrama de flujo para obtener el documento a firmar.

Figura 4. Muestra un diagrama de flujo del proceso para obtener la identidad del usuario.

Figura 5. Muestra un diagrama de flujo para identificar el usuario.

5

Figura 6. Muestra un diagrama de flujo para obtener los videos de firma.

Figura 7. Muestra un diagrama de flujo para mostrar el documento a firmar.

10 **Figura 8.** Muestra un diagrama de flujo para realizar firma autógrafa.

Figura 9. Muestra un diagrama de flujo para crear archivo de la firma.

Figura 10. Muestra un diagrama de flujo para validar información.

15

Figura 11. Muestra un diagrama de flujo para validar la integridad de la firma.

Figura 12. Muestra un diagrama de flujo para comparar la información de archivos obtenidos.

20

Figura 13. Muestra un diagrama de flujo para certificar la firma y distribuir el documento.

Figura 14. Muestra un diagrama esquemático del sistema.

25

DESCRIPCIÓN DE LA INVENCION

A continuación, se hará referencia a detalles a las modalidades ejemplares, las cuales se ilustran en los dibujos anexos. Las implementaciones que se describen de las modalidades ejemplares no representan todas las implementaciones contenidas en la presente descripción, estas son simplemente ejemplos de aparatos y métodos

30

consistentes con aspectos relacionados con la presente descripción como se indica en las reivindicaciones adjuntas. Las terminologías utilizadas en esta memoria descriptiva son solo para describir modalidades particulares, pero no para limitar la presente descripción.

5

La figura 1 muestra el diagrama de flujo del método para realizar para realizar la firma autógrafa digital, dicho método de implementa en un dispositivo móvil de un usuario que tiene interés de firmar algún documento de forma digital, esto por medio de una interfaz y que se lleva a cabo en la etapa (100), en donde se realiza una
10 verificación de que la interfaz se encuentre el disponible en el dispositivo móvil, que en el caso de que se encuentra la interfaz entonces se puede recibir una notificación para firmar un documento, una vez que se confirma que se desea realizar la firma autógrafa digital, entonces se realiza un procesamiento de la información de identificación.

15 Posteriormente, en la etapa (200) se realiza el procesamiento de la firma autógrafa digital, la cual se lleva a cabo con el dedo del usuario y además se realiza un video del momento en que se traza la firma en la pantalla del dispositivo móvil, esto como una de las medidas de seguridad, también realizando otro video en el cual se graba la lectura del usuario del documento que ha firmado, por lo que esta
20 característica define parte de la seguridad de la firma del documento.

En la etapa (300) se lleva a cabo la parte final del proceso, en la cual, los datos que se obtuvieron por medio del dispositivo móvil, son enviados a los servidores que van a garantizar el la autenticidad de la firma, por lo que en esta etapa se lleva a cabo
25 el procesamiento de la información obtenida, se verifica si es que hay otras personas adicionales deben firmar el documento, por lo que en el caso de que otras personas deban firmar, entonces se realizan dichas firmas y posteriormente se adicionan dos mecanismos de seguridad adicionales, con los cuales consisten en agregar un Hash y un Timestamp a los archivos generados, se obtienen constancias de conservación y
30 se envía, los archivos al usuario firmante y a la institución a la que se le firma. En donde estas instituciones se encuentran entro otras como las empresas FinTech; los

bancos, en los cuales es ideal para procesos de originación, captación y colocación, con esta firma autógrafa digital se pueden firmar: contratos, instrucciones, órdenes, pagares, solicitudes, entre otros documentos; aseguradoras, en las cuales aplica para cualquier tipo de seguros, y permite firmar solicitudes, siniestros, reembolsos, servicios de proveedores y más; agencias aduanales y de comercio exterior; comercializadoras; arrendadoras; así como las empresas con necesidades de certeza jurídica en ambientes móviles y virtuales, como las casas de bolsa, en donde se pueden firmar contratos, instrucciones, ordenes, solicitudes, retiros, etc.

La figura 2 muestra el diagrama de flujo correspondiente a la obtención de la información de la etapa (100) de la figura 1, en donde se la etapa (110) se lleva a cabo la notificación al usuario del dispositivo móvil que tiene un documento en espera para realizar la firma autógrafa digital, en donde al ser aceptada, se realiza la etapa (130), en la cual se lleva a cabo el procesamiento de la información personal del usuario para determinar si es realmente quien debe de realizar la firma del documento, para esto se determina en la etapa (150) si la persona que se encuentra con el dispositivo móvil es la misma persona que debe realizar la firma autógrafa digital, por lo que si el resultado de esta determinación es que no es la misma persona, entonces se cancela el proceso, sin embargo, en el caso de que se determine que si es la misma persona, entonces se valida la información y desarrolla la etapa (200) de la figura 1.

La figura 3 muestra una modalidad del diagrama de flujo para que el usuario del dispositivo móvil pueda obtener el documento a firmar, de tal manera que la etapa (111) obtiene la información del dispositivo móvil para de esta manera determinar que la interfaz para realizar la firma autógrafa digital se realiza adecuadamente, por lo que en la etapa (112) se determina si se tiene la interfaz para realizar la firma autógrafa digital en el dispositivo móvil, que en el caso de que no se cuente con dicha interfaz, entonces, se realiza la etapa 115 en la cual se descarga y se instala la interfaz.

Cuando se cuenta con dicha interfaz en el dispositivo móvil, entonces en la etapa (112) se determina que, si se cuenta con la interfaz realizándose ahora la etapa

(113), en donde se determina que, si se ha recibido un mensaje tipo SMS con la clave para poder obtener el documento a firmar, si en esta determinación no se tiene el mensaje, entonces se realiza la etapa (114), en el cual se espera o notifica el mensaje tipo SMS. En el caso de que en la etapa (113) se determina que si se tiene el mensaje, entonces en la etapa (116) se determina si se ha recibido un vínculo a un documento, con lo cual se realiza para verificar si el usuario ya cuenta con el documento a firmar, que en el caso de que no se cuente con el documento, entonces en la etapa (117) se mantiene un tiempo en espera para verificar si en ese tiempo se tiene el vínculo al documento esperado o se realiza una notificación para informar que dicho documento no se ha recibido, para así pasar nuevamente a la etapa (116), en donde en el caso de que se tenga el vínculo al documento a firmar, entonces se realiza la etapa (118).

En la etapa (118), el usuario puede por medio del dispositivo móvil tener acceso al documento esperado, para lo cual abre el vínculo recibido e ingresa la clave de acceso para poder tener el documento en el dispositivo móvil, una vez que se ha realizado el paso (118), se determina si el ingreso es correcto, lo cual se realiza en la etapa (119), que en el caso de que no se ha ingresado correctamente, se realiza la etapa (120), en la cual se tiene la oportunidad de realizar nuevamente el intento de capturar los datos para poder ingresar correctamente, y si por alguna razón no se ha podido realizar el ingreso adecuadamente se realiza la etapa (121), en donde se cancela el proceso después de tres intentos para obtener el documento a firmar. En el caso de que en la etapa (119) se determina que el ingreso si ha sido el correcto, entonces se realiza la etapa (122), en la cual el usuario acepta el aviso de privacidad, para después en la etapa (123) la interfaz muestra una serie de instrucciones que el usuario debe seguir para poder usar la interfaz y realizar la firma autógrafa digital.

La figura 4 muestra un diagrama de flujo del proceso para obtener la identidad del usuario que desea firmar el documento, esta es una medida de seguridad para evitar la suplantación de identidad y así evitar que una tercera persona realice la firma a nombre del interesado, de tal manera que después de realizar la etapa (123) (de la figura 3), se realiza la etapa (131) en la cual se le solicita al usuario que por medio del

dispositivo móvil al usar la interfaz para la firma autógrafa digital, escanee su identificación con fotografía (ID), que podría ser como ejemplo la credencial del INE. Una vez que se ha realizado la etapa de escanear el ID del usuario, entonces se realiza la etapa (132), en la cual la interfaz de la FAD obtiene la información del ID del usuario, la cual se procesó por medio de un reconocedor de caracteres (OCR) y poder así determinar en la etapa (133) si la información es correcta, cuando la información no es correcta, entonces se regresa a la etapa (133) nuevamente, pasando por la etapa (134) en donde se lleva a cabo la corrección de la información, para así determinar si la información es correcta, esto con el fin de realizar nuevamente el escaneo del ID del usuario.

Cuando se determina que la información es correcta, entonces se lleva a cabo la etapa (135), en esta etapa se obtiene la huella dactilar del usuario por medio de la interfaz en el dispositivo móvil, mientras que en la etapa (136) se le indica al usuario que se tome una selfie, esto con el fin de poder identificar si en realidad el usuario es la misma persona que la del ID que se escaneo en la etapa (131), y con lo cual se va dando seguridad al proceso de identificación para poder realizar la firma autógrafa digital del documento, para finalmente en la etapa (137) se realiza una comparación de la selfie que se acaba de obtener con la fotografía del documento ID del usuario obtenida en la etapa (131), finalmente en la etapa (138) se determina si la persona que se ha identificado por medio de la selfie es la misma a la del documento ID, en el caso de que no sea la misma persona, entonces se realiza la etapa (139) en donde se cancela el proceso y se avisa que la persona no es la misma, mientras que en el caso de que la persona si sea la misma, entonces el proceso continua en la etapa (191) de la figura 5, de tal manera que con el procesamiento de esta información se lleva a cabo la etapa (150) de la figura 2.

La figura 5 muestra un diagrama de flujo con el cuál se identifica el usuario que pretende firmar el documento, el cual se realiza al determinarse en la etapa (150) de la figura 2 que la persona que desea firmar el documento es la misma persona que se ha identificado con el ID que ha proporcionado, de tal forma que al determinarse en

(150) que si es la misma persona, entonces se lleva cabo la etapa (191), en donde se realiza una validación de la huella dactilar y la información de ID del usuario con la institución que la emite, por lo que el dispositivo móvil establece una comunicación a un servidor de dicha institución, por lo que la institución del ID recibe dicha información proporcionada por el dispositivo móvil y la valida, esto se lleva a cabo en la etapa (192).

Una vez que la institución que emitió el ID del usuario valida la información la retorna al dispositivo móvil en el cual, por medio de la interfaz, se realiza la etapa (193), en la cual se determina que dicha información sea correcta, que en el caso de que no sea correcta, entonces en la etapa (194) se cancela el proceso. Por otro lado, en el caso de que la información si sea la correcta, entonces se realiza la etapa (195), en la cual se da aviso al usuario firmante que puede continuar con la firma.

Una vez que se ha llevado a cabo la validación de la información del usuario firmante, entonces se procede a realizar el proceso para firmar el documento. De esta manera la figura 6 muestra un diagrama de flujo para realizar la firma del documento en la cual se incorporan los videos del momento de realizar la firma, por lo que en el paso (210) se muestra la etapa en la cual al usuario se le presentan los pasos que debe seguir para realizar la firma así como el documento a firmar, esto por medio de la interfaz FAD, para posteriormente en el paso (220) se activa una herramienta del dispositivo móvil para poder realizar una videograbación, y después en el paso (230) se determina si el usuario está satisfecho con la firma realizada, en el caso de que no se encuentre satisfecho, entonces regresa a la etapa (220) para repetir el proceso. Pero si de (230) el usuario está satisfecho, entonces en la etapa (240), se activa nuevamente la herramienta de videograbación y se le solicita al usuario se coloque frente a la pantalla al mismo tiempo que se le muestra un texto que deberá de leer fuerte y claro, en donde el texto leído compromete al usuario cumplir el acuerdo que está adquiriendo en el documento (script de acuerdo), por lo que en la etapa (250) el usuario lee el texto del script de acuerdo mientras la interfaz captura el video correspondiente a dicha lectura. Una vez realizada la lectura, el paso (260) determina si el usuario está satisfecho con el video grabado, que en el caso de que no esté

satisfecho, entonces regresa a la etapa (240) para repetir le proceso nuevamente, cuando el usuario está satisfecho después de la determinación en la etapa (260), entonces se realiza la etapa (270), que es en donde la interfaz FAD realiza el proceso de generación de los archivos correspondientes.

5

La figura 7 muestra un diagrama de flujo por medio del cual se realizan las etapas para mostrar el documento a firmar, de esta forma, en la etapa (211) se realiza al desarrollarse la etapa (210) de la figura 6, por lo tanto, la etapa (211) se genera a partir del resultado de la etapa (195) de la figura 5, en donde, por medio de la interfaz, se le aviso al usuario que podía realizar la firma, entonces en la etapa (211) va a presentar al usuario los pasos que debe realizar para poder hacer la firma autógrafa digital en el documento deseado, y una vez que se en usuario conoce los paso que va a realizar, entonces la desarrolla la etapa (212) se le muestra al usuario el documento a firmar, para posteriormente en la etapa (213) se muestra las partes del documento a firmar, las cuales el usuario va aceptando al darle en la interfaz FAD tap a los apartados en donde se requiere su firma, para finalmente en la etapa (214) el usuario acepta la totalidad del documento a firmar al dar tap al final del documento.

Al finalizarla etapa (214), se pasa a la etapa (220) de la figura 6 y al realizar la etapa (220), la cual en la figura 8 muestra las etapas correspondientes al proceso de activación de una herramienta para la videograbación, por lo tanto después de realizar la etapa (214) de la figura 7, se lleva a cabo la etapa (221) de la figura 8, en donde se inicializa el proceso de la herramienta de videograbación, con la cual se va a tomar los videos para la firma correspondiente del documento a firmar, por lo que una vez iniciado el proceso de video, se realiza la etapa (222) en la cual se le solicita al usuario colocarse frente a la pantalla del dispositivo móvil para hacer el reconocimiento del rostro del usuario, cuando se ha identificado el rostro, entonces la interfaz FAD permite al usuario realizar si firma autógrafa como el del documento ID que presento en la (131) de la figura 4, al mismo tiempo que el usuario realiza el trazo de su firma autógrafa sobre la pantalla, el dispositivo móvil graba en la etapa (223) al usuario en video mientras está firmando sobre la pantalla del dispositivo móvil, por lo que después

de terminar la firma, la interfaz muestra al usuario el video de si mismo con el autografo manuscrito en el dispositivo móvil, lo cual se lleva a cabo en la etapa (224), para así continuar en la etapa (230) de la figura 6.

5 La figura 9 muestra el diagrama de flujo para crear los archivos necesarios de la firma autógrafa digital (FAD) la cual se realiza al determinarse que el usuario se encuentra satisfecho con el video de texto leído de la etapa (260) de la figura 6 , iniciándose así la etapa (271), en donde a través de la interfaz se muestran los elementos de la firma al usuario en el dispositivo móvil, los cuales consisten en la
10 firma digital, video firma digital y video firma por voz, para que después el usuario en la etapa (272) acepta concluir el proceso.

Una vez que el usuario ha aceptado concluir con el proceso, entonces en la etapa (273) se obtiene del dispositivo móvil los datos de: geolocalización; UID; fecha;
15 hora; nombre del dispositivo; marca; modelo; y versión de la interfaz, para así realizar la etapa (274) en la cual se generan los archivos de extensión. FAD1 encriptado que contiene toda la información del documento firmado. Posteriormente en la etapa (275), se envía el archivo .FAD1 a un servidor "Back-en FAD" en donde se lleva a cabo el procesamiento de la información, posteriormente, en la etapa (276) se borra toda la
20 información generada durante el proceso de la firma autógrafa digital en el dispositivo móvil.

La figura 10 muestra un diagrama de flujo con el cuál se realiza el proceso de validación de la información, el cual corresponde al proceso realizado en la etapa (300)
25 de la figura 1, por lo tanto; de la etapa (275) de la figura 9, se lleva a cabo la etapa (310), en la cual se recibe la información y se valida el proceso de la firma, realizándose posteriormente la etapa (320) en donde se compara la información obtenida de los archivos que fueron generados, con la información del ID del usuario ocupado en la etapa (131) de la figura 4, una vez comparados los datos, se realiza la etapa (330), en
30 la cual se determina si hay más personas que van a firmar el documento, que en en el caso de que si hay más personas se repite el proceso desde la etapa (320) hasta que

todos los firmantes han firmado, en el caso de que ya no hay más personas para firmar, entonces se realiza la etapa (340), que es en donde se generan los archivos correspondientes y se obtiene la constancia de conservación, para posteriormente realizar la etapa (350), en la cual los archivos .FAD y .PDF son enviados a la institución que los emitió así como a cada uno de los firmantes, para posteriormente realizar la etapa (360) en la cual, la institución que emitió el documento para firma, así como cada uno de los firmantes, reciben una copia del documento firmado en formato .FAD y .PDF, esto con el fin de que dichos documentos sean resguardados y posteriormente puedan ser consultados, dichos documentos son enviados a los firmantes por correo electrónico certificado, mientras que la institución los recibe en su infraestructura.

La figura 11 muestra un diagrama de flujo para validar la integridad de la firma que corresponde a la etapa (310) de la figura 10, por lo que a partir de la etapa (195) (de la figura 5), se realiza la etapa (311), en la cual se la información generada es recibida por el servidor “Back-end FAD”, se des-encrpta y posteriormente se valida la integridad de la información, y al terminar, se compara la firma recabada por el dispositivo con la firma del documento ID del firmante, una vez comparada dicha información, entonces se determina si la firma es la misma, lo cual se realiza en la etapa (312), en el caso de que no sea la misma firma, entonces se realiza la etapa (314), en donde se cancela el proceso y se da aviso al firmante.

La figura 12 muestra un diagrama de flujo para comparar la información de archivos obtenidos, por lo que una vez que en la etapa (313) de la figura 11 se determina si la firma es la misma, entonces en la etapa (321) se compara por medio de biometría facial un trozo aleatorio de la frame de video firma digital con la fotografía ID del usuario, para determinar en (322) si es la misma persona, que en el caso de que no sea la misma persona, entonces se cancela el proceso en la etapa (323) y se da aviso al firmante, mientras que si de (322) se determina que el firmante es la misma persona, entonces se compara en la etapa (324) el videoacuerdo con foto de ID por biometría facial, un frame aleatorio de la videofirma por voz con la fotografía del ID, para que con dicha información en la etapa (325) se realiza una segunda

determinación para identificar si es la misma persona la que está firmando, que en el caso de que no sea la misma persona, entonces en la etapa (326) se cancela el proceso y se da aviso al firmante.

5 La figura 13 muestra un diagrama de flujo para certificar la firma y distribuir el documento, para lo cual este proceso se realiza del proceso de la etapa (330) de la figura 10, en donde después de la etapa (325) de la figura 12, se realiza la etapa (331), en el cual se crea un HASH único e irrepetible del archivo, para posteriormente, en la etapa (332) el HASH obtenido se convierte en un ASN.1 estándar, el cuál es enviado
10 a un servidor de un tercero el cual es un servidor de una institución certificadora, por lo que en la etapa (333) se la institución certificada genera una constancia de conservación, y en la etapa (334) se guarda la constancia de certificación en una base de datos de la institución certificada. Cuando la institución certificada regresa la información correspondiente, en la etapa (335) en donde con el archivo .FAD1; el
15 HASH y la constancia de conservación, se crea un archivo de nombre único de extensión .FAD. una vez que se obtiene el archivo .FAD, en la etapa 336 se crea un archivo .PDF, el cuál es una representación gráfica del archivo .FAD, mientras que en la etapa (337), el archivo .FAD es cifrado para incrementar la seguridad, dicho cifrado se realiza con AES (256) y el archivo .PDF el cual es protegido con un código de
20 seguridad.

La figura 14 muestra un diagrama esquemático del sistema (400), en donde muestra la integración del sistema, el cual se observa se encuentra conformado por el dispositivo móvil (402), el cual es el dispositivo de usuario en donde se va a realizar la
25 firma autógrafa digital (FAD) por medio de la interfaz que se encuentra en el dispositivo (402), mientras que un servidor de administración (401) es el encargado de administrar el funcionamiento del sistema, mientras que en (403) se muestra un portal de usuario final, el sistema cuenta con servidores adicionales los cuales se encargan de dar la validación y certificación del proceso por lo que en (404) se observa un servidor back-
30 end en donde se va a procesar parte de la información, también se observa un servidores de emisor del documento ID en cual en su momento, el dispositivo móvil envía la

información a este servidor para la validación de la información de los datos del documento de identificación del usuario y así al regresar la información al dispositivo móvil 402, este continua con el proceso, por lo que al final se manda la información con un tercer servidor, en donde se lleva a cabo un proceso para obtener una
5 constancia de conservación, y este a su vez guarda la información en una base de datos, el anterior sistema se encuentra configurado para funcionar de acuerdo a la implementación del método que se desarrolla para realizar la firma autógrafa digital.

Así mismo y de conformidad con el método ampliamente descrito en esta
10 memoria descriptiva, se desarrolla un medio legible por computadora el cual contiene el método ya mencionado e ilustrado en las figuras que acompaña la presente descripción.

Con lo anterior, se han descrito las modalidades preferidas de la presente
15 descripción con referencia a las figuras adjuntas, sin limitarse a lo anterior, por lo que una persona con habilidad en el arte puede modificar o encontrar alternativas que estén dentro de la cercanía de las reivindicaciones adjuntas y se deberá de entender que caerán naturalmente bajo la cercanía técnica de la presente descripción.

REIVINDICACIONES

1. Un método en un sistema para generar una firma autógrafa digital caracterizado el método por realizar los pasos de:

5

notificar a un usuario, por medio de una interfaz de un dispositivo móvil, que tiene un documento que, al ser aceptado, se le debe incorporar una firma autógrafa digital;

10

escanear, por medio de la interfaz del dispositivo móvil, un documento de identificación del usuario que va a firmar;

determinar, por medio de la interfaz del dispositivo móvil, si la información que fue escaneada es correcta;

15

obtener, por medio de la interfaz del dispositivo móvil, la huella dactilar del usuario que va a firmar;

20

tomar, por medio de la interfaz del dispositivo móvil, una selfie del usuario que va a firmar, esto como un comprobante de vida;

25

comparar, por medio de la interfaz del dispositivo móvil, la selfie con la fotografía del documento de identificación del usuario que va a firmar, esto para verificar que es la misma persona y evitar que una tercera persona firme a nombre del usuario;

30

enviar, por medio del dispositivo móvil a un servidor de la institución emisora del documento de identificación, los datos recabados para validar la información proporcionada por el usuario;

obtener, por medio de la interfaz del dispositivo móvil, el documento a firmar, activando a su vez una herramienta para videograbar el trazo de la firma del usuario sobre la pantalla del dispositivo móvil, así como una videograbación con la lectura del texto en donde se compromete a cumplir el acuerdo que se está adquiriendo;

mostrar, por medio de la interfaz del dispositivo móvil, el autógrafo manuscrito, así como los elementos de la firma en la pantalla del dispositivo móvil;

crear, por medio de la interfaz del dispositivo móvil, archivos encriptados con la información contenida y enviar dicha información a un servidor back-end FAD;

comparar, por medio del servidor Back-end FAD la información de los archivos contenidos con la información del documento de identificación del usuario;

comparar, por medio del servidor Back-end FAD, usando biometría facial, si el usuario y el documento de identificación son la misma persona;

crear, por medio del servidor Back-end FAD, un hash unido del archivo y convertir dicho hash en un estándar ASN.1 para enviarlo a un tercer servidor para obtener una constancia de certificación, guardando el tercer servidor una copia de la constancia de certificación en una base de datos;

crear, por medio del servidor Back-end FAD un archivo de nombre único de extensión FAD y posteriormente en base al archivo con extensión FAD se crea un archivo con extensión .PDF, así mismo, el archivo FAD se cifra y el archivo .PDF se protege con un código de seguridad;

enviar, por medio del servidor Back-end FAD los archivos FAD y .PDF a la institución que los emitió y al menos a un usuario firmante.

- 5 2. El método en un sistema para generar una firma autógrafa digital como el de la reivindicación 1 caracterizado además por el paso de cancelar el proceso por medio de la interfaz del dispositivo móvil, cuando despues de notificar al usuario del documento que se le debe de incorporar la firma autógrafa, el usuario comete tres fallas en el intento de ingreso.
- 10 3. El método en un sistema para generar una firma autógrafa digital como el de la reivindicación 1 caracterizado además por el paso de cancelar el proceso por medio de la interfaz del dispositivo móvil, y avisar cuando en el paso de comparar la selfie con la fotografía de ID se determina que la persona de la selfie no es la misma persona de la ID.
- 15 4. El método en un sistema para generar una firma autógrafa digital como el de la reivindicación 1 caracterizado además por el paso de cancelar el proceso por medio de la interfaz del dispositivo móvil, cuando la información con la institución emisora del documento de identificación no es correcta, en el caso contrario, se avisa al firmante que puede continuar con la firma.
- 20 5. Un sistema para generar una firma autógrafa digital que comprende un dispositivo móvil; un servidor de institución emisora de documento de identificación; un servidor Back-end FAD; un tercer servidor que emite un certificado de conservación; caracterizado porque el dispositivo móvil, por medio de una interfaz se configura para:
- 25 notificar a un usuario que tiene un documento, que, al ser aceptado, se le debe incorporar una firma autógrafa digital;
- 30 escanear, un documento de identificación del usuario que va a firmar;
- 30 determinar, si la información que fue escaneada es correcta;

obtener, la huella dactilar del usuario que va a firmar;

tomar, una selfie del usuario que va a firmar, esto como un comprobante de vida;

5

comparar, la selfie con la fotografía del documento de identificación del usuario que va a firmar, esto para verificar que es la misma persona y evitar que una tercera persona firme a nombre del usuario;

10

enviar a un servidor de la institución emisora del documento de identificación, los datos recabados para validar la información proporcionada por el usuario;

15

obtener, el documento a firmar, activando a su vez una herramienta para videograbar el trazo de la firma del usuario sobre la pantalla del dispositivo móvil, así como una videograbación con la lectura del texto en donde se compromete a cumplir el acuerdo que se está adquiriendo;

20

mostrar, el autógrafo manuscrito, así como los elementos de la firma en la pantalla del dispositivo móvil;

crear, archivos encriptados con la información contenida y enviar dicha información a un servidor back-end FAD;

25

el servidor Back-end FAD se configura para:

comparar la información de los archivos contenidos con la información del documento de identificación del usuario;

30

comparar usando biometría facial, si el usuario y el documento de identificación son la misma persona;

crear un hash unido del archivo y convertir dicho hash en un estándar ASN.1 para enviarlo a un tercer servidor para obtener una constancia de certificación, guardando el tercer ser servidor una copia de la constancia de certificación en una base de datos;

5

crear un archivo de nombre único de extensión .FAD y posteriormente en base al archivo con extensión .FAD se crea un archivo con extensión .PDF, así mismo, el archivo .FAD se cifra y el archivo .PDF se protege con un código de seguridad;

10

enviar los archivos. FAD y .PDF a la institución que los emitió y al menos a un usuario firmante.

15

- 6.** El sistema para generar una firma autógrafa digital como el de la reivindicación 1 caracterizado además porque el dispositivo móvil, por medio de la interfaz, cancela el proceso, cuando despues de notificar al usuario del documento que se le debe de incorporar la firma autógrafa, el usuario comete tres fallas en el intento de ingreso.

20

- 7.** El sistema para generar una firma autógrafa digital como el de la reivindicación 1 caracterizado además porque el dispositivo móvil, por medio de la interfaz, cancela el proceso y avisa cuando en el paso de comparar la selfie con la fotografía de ID se determina que la persona de la selfie no es la misma persona de la ID.

25

- 8.** El sistema para generar una firma autógrafa digital como el de la reivindicación 1 caracterizado además porque el dispositivo móvil, por medio de la interfaz, cancela el proceso cuando la información con la institución emisora del documento de identificación no es correcta, en el caso contrario, se avisa al
- firmante que puede continuar con la firma.

30

9. Un medio legible por computadora que contiene un método para generar una firma autógrafa digital que se realiza un sistema caracterizado por realizar los pasos de:

5 notificar a un usuario que tiene un documento que, al ser aceptado, se le debe incorporar una firma autógrafa digital;

escanear un documento de identificación del usuario que va a firmar;

10 determinar si la información que fue escaneada es correcta;

obtener, por medio de la interfaz del dispositivo móvil, la huella dactilar del usuario que va a firmar;

15 tomar una selfie del usuario que va a firmar, esto como un comprobante de vida;

comparar la selfie con la fotografía del documento de identificación del usuario que va a firmar, esto para verificar que es la misma persona y evitar que una tercera persona firme a nombre del usuario;

20 enviar a un servidor de la institución emisora del documento de identificación, los datos recabados para validar la información proporcionada por el usuario;

25 obtener el documento a firmar, activando a su vez una herramienta para video grabar el trazo de la firma del usuario sobre la pantalla del dispositivo móvil, así como una videograbación con la lectura del texto en donde se compromete a cumplir el acuerdo que se está adquiriendo;

30 mostrar el autógrafo manuscrito, así como los elementos de la firma en la pantalla del dispositivo móvil;

crear archivos encriptados con la información contenida y enviar dicha información a un servidor back-end FAD;

5 comparar la información de los archivos contenidos con la información del documento de identificación del usuario;

comparar usando biometría facial, si el usuario y el documento de identificación son la misma persona;

10 crear un hash unido del archivo y convertir dicho hash en un estándar ASN.1 para enviarlo a un tercer servidor para obtener una constancia de certificación, guardando el tercer ser servidor una copia de la constancia de certificación en una base de datos;

15 crear un archivo de nombre único de extensión .FAD y posteriormente en base al archivo con extensión .FAD se crea un archivo con extensión .PDF, así mismo, el archivo .FAD se cifra y el archivo .PDF se protege con un código de seguridad;

20 enviar los archivos .FAD y .PDF a la institución que los emitió y al menos a un usuario firmante.

RESUMEN

La presente invención da a conocer un método, un sistema y un medio legible por computadora para que un usuario por medio de una dispositivo móvil que contiene una interfaz, pueda realizar la firma de documentos por medio de una firma autógrafa digital, esta firma cuenta que pleno valor jurídico y se puede firmar documentación de empresas Fin Tech, bancos, aseguradoras, agencias aduanales y de comercio exterior, comercializadoras, arrendadoras, y empresas con necesidades de certeza jurídica en ambientes móviles y virtuales, en donde el dispositivo móvil por medio de la interfaz notifica al menos a un usuario de que tiene un documento que firmar, se realiza el procesamiento de la firma de documento al verificar la identidad del usuario por medio de un documento de identificación, y finalmente procesa la firma y verifica la identidad del usuario al comprobar, por medio de biometría facial una foto obtenida por el dispositivo móvil con la fotografía del documento de identificación del usuario.

15

20

25

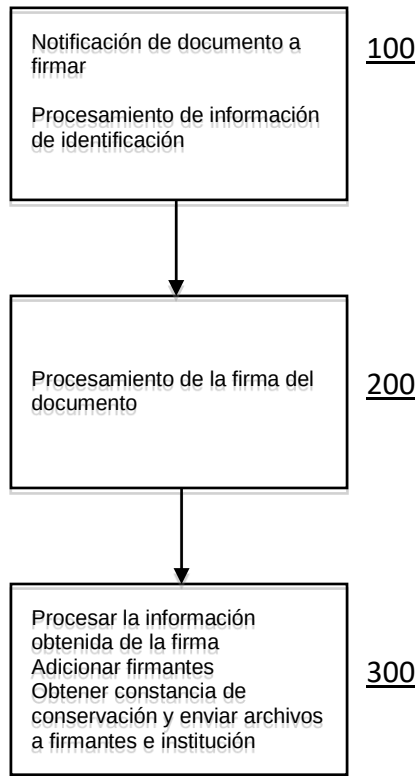


Fig. 1

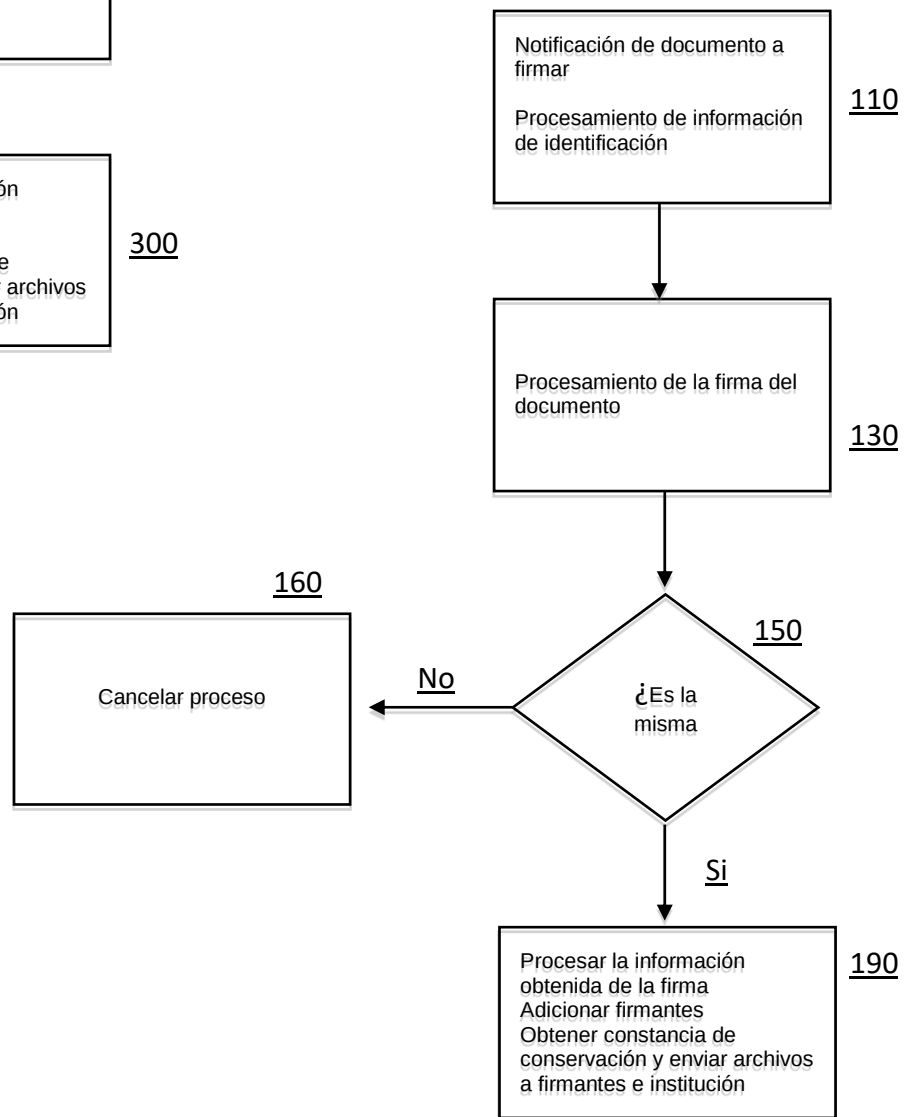


Fig. 2

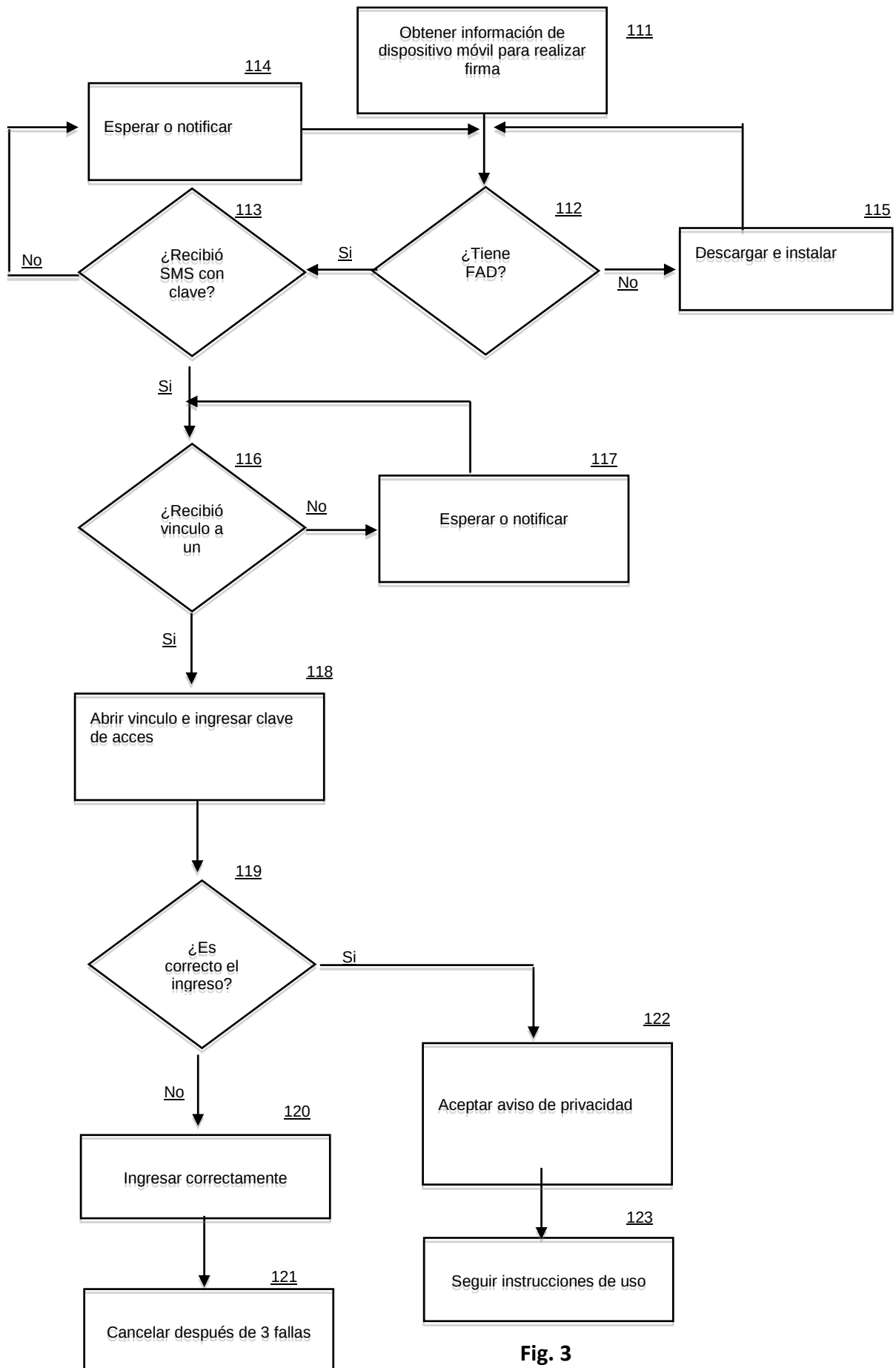
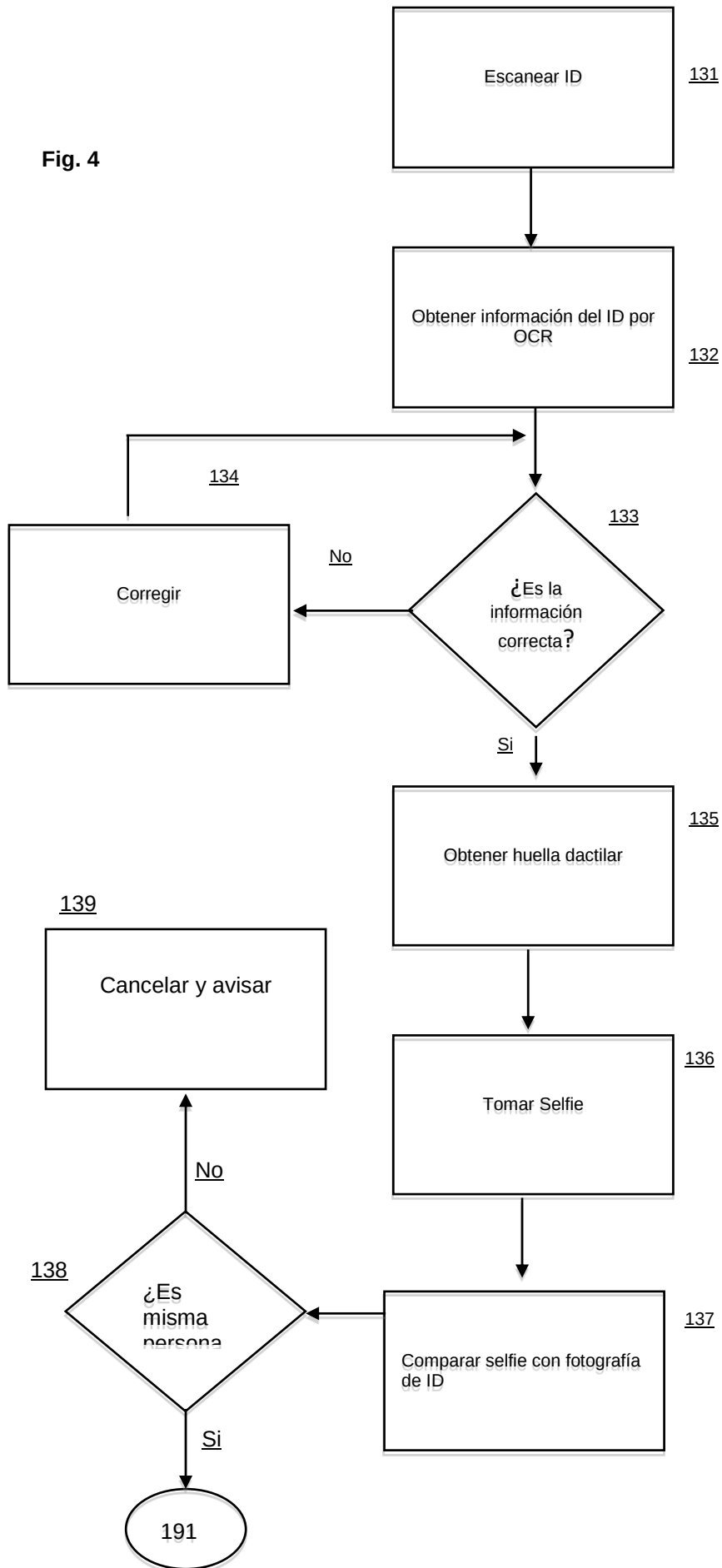


Fig. 3

Fig. 4



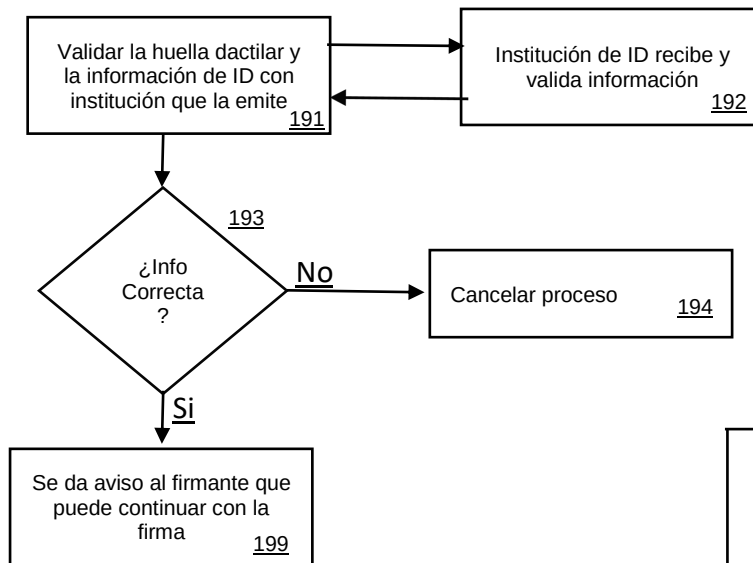


Fig. 5

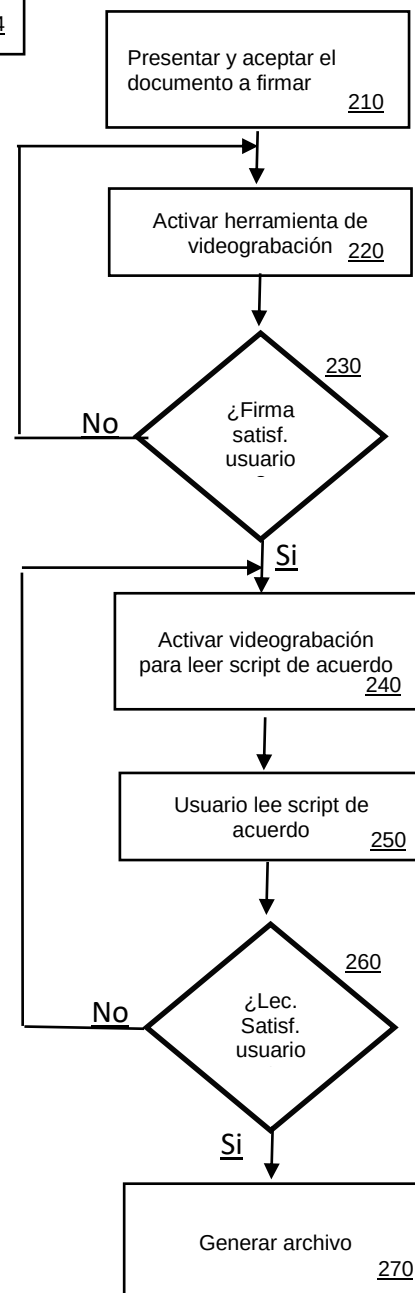


Fig. 6

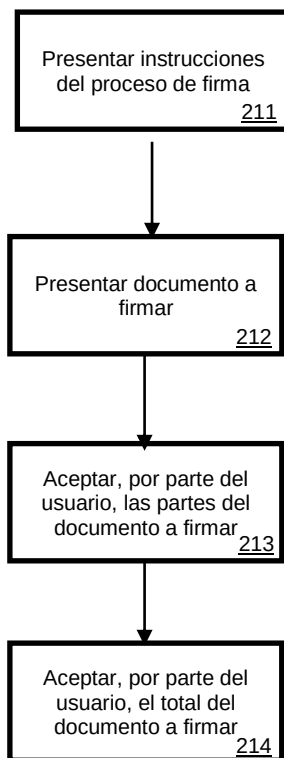


Fig. 7

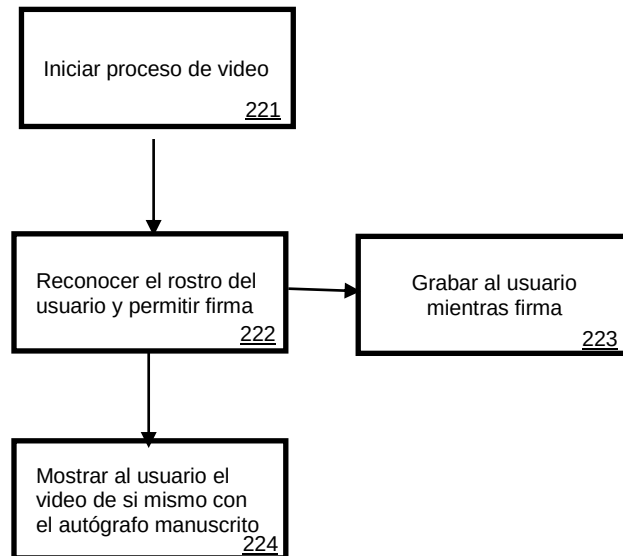


Fig. 8

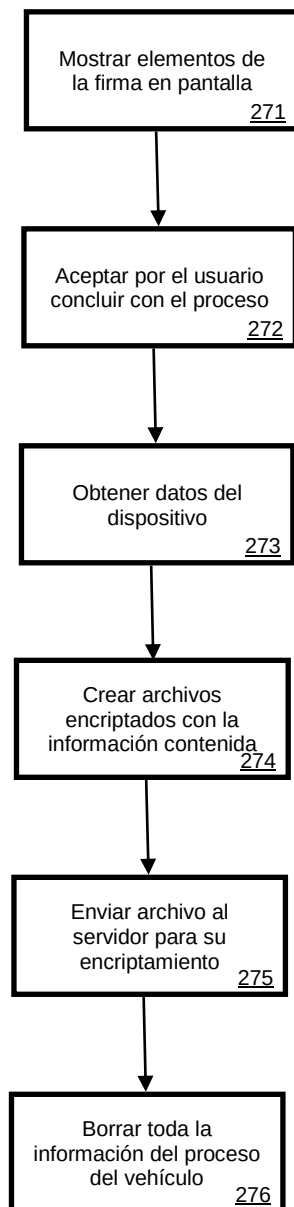


Fig. 9

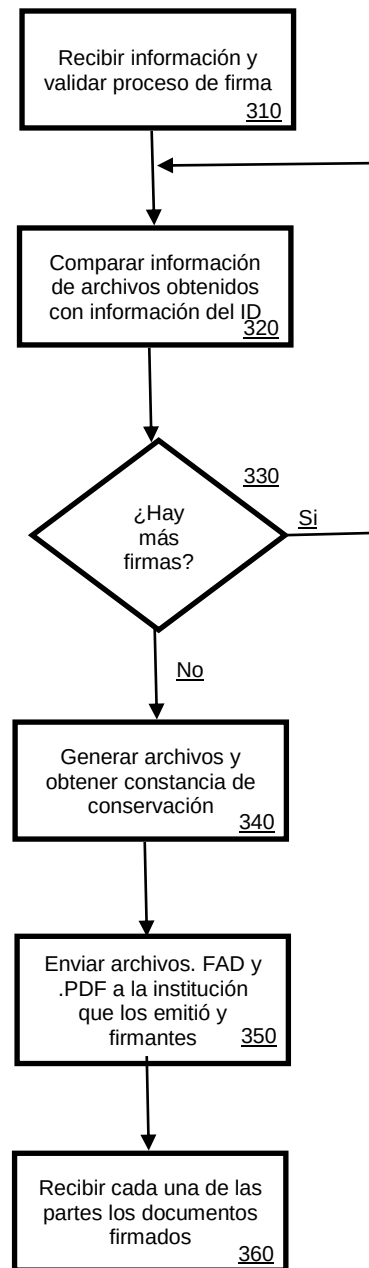


Fig. 10

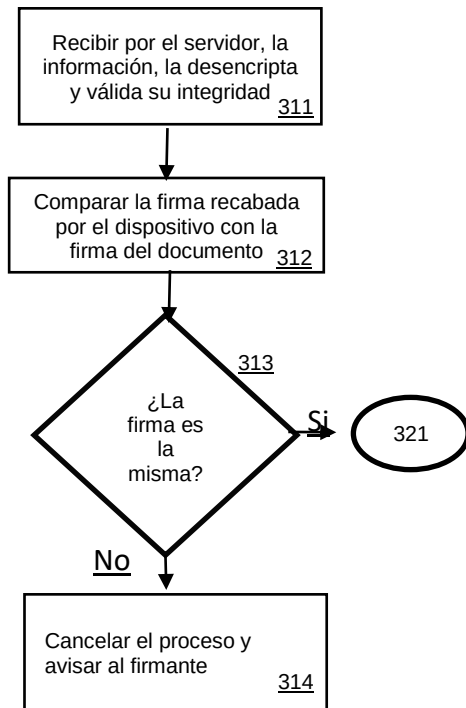


Fig. 11

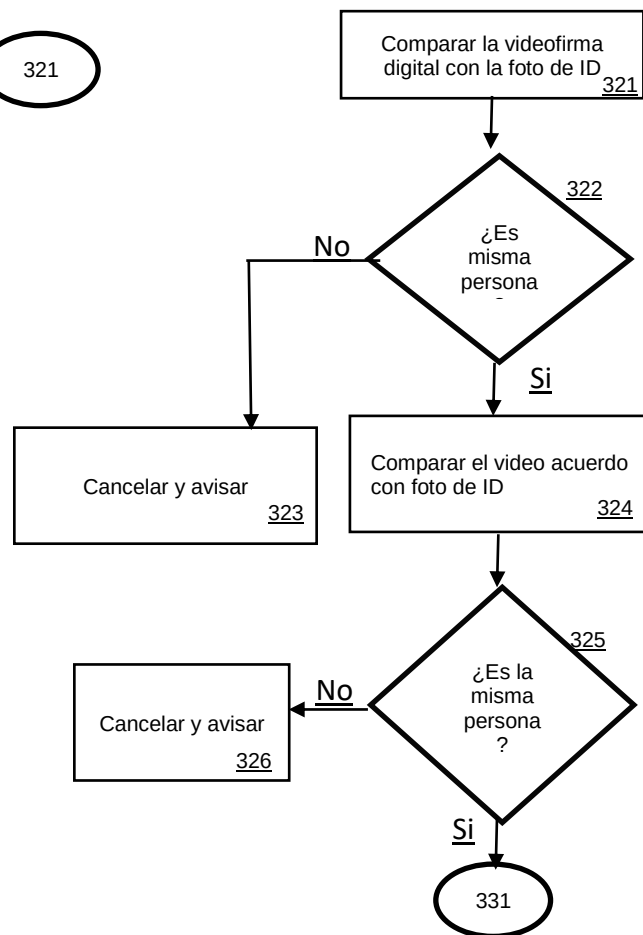


Fig. 12

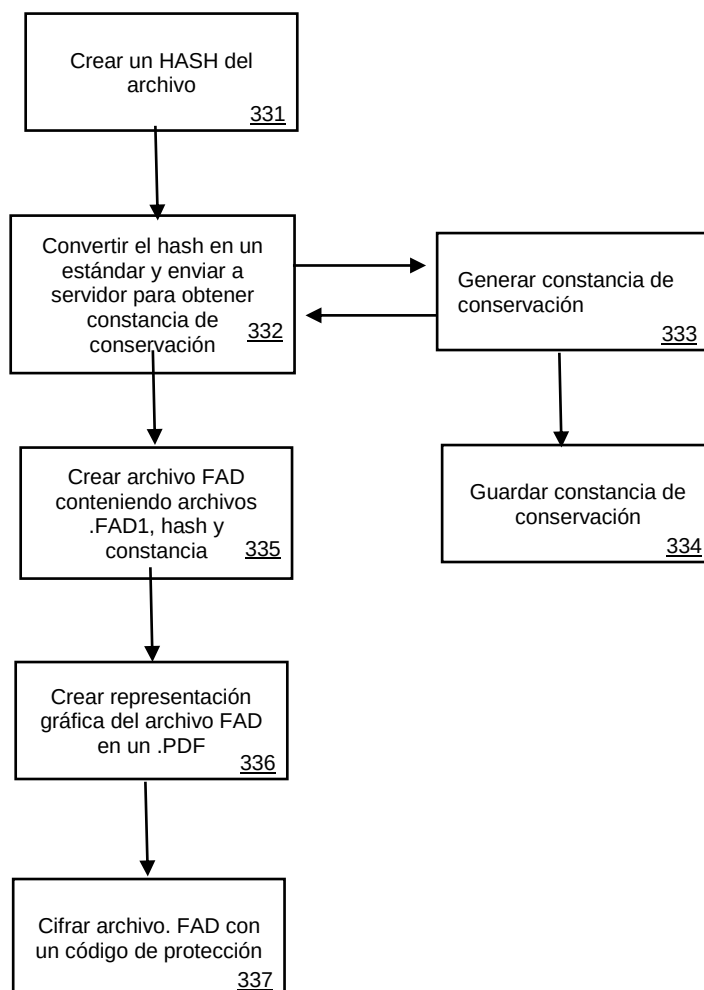


Fig. 13

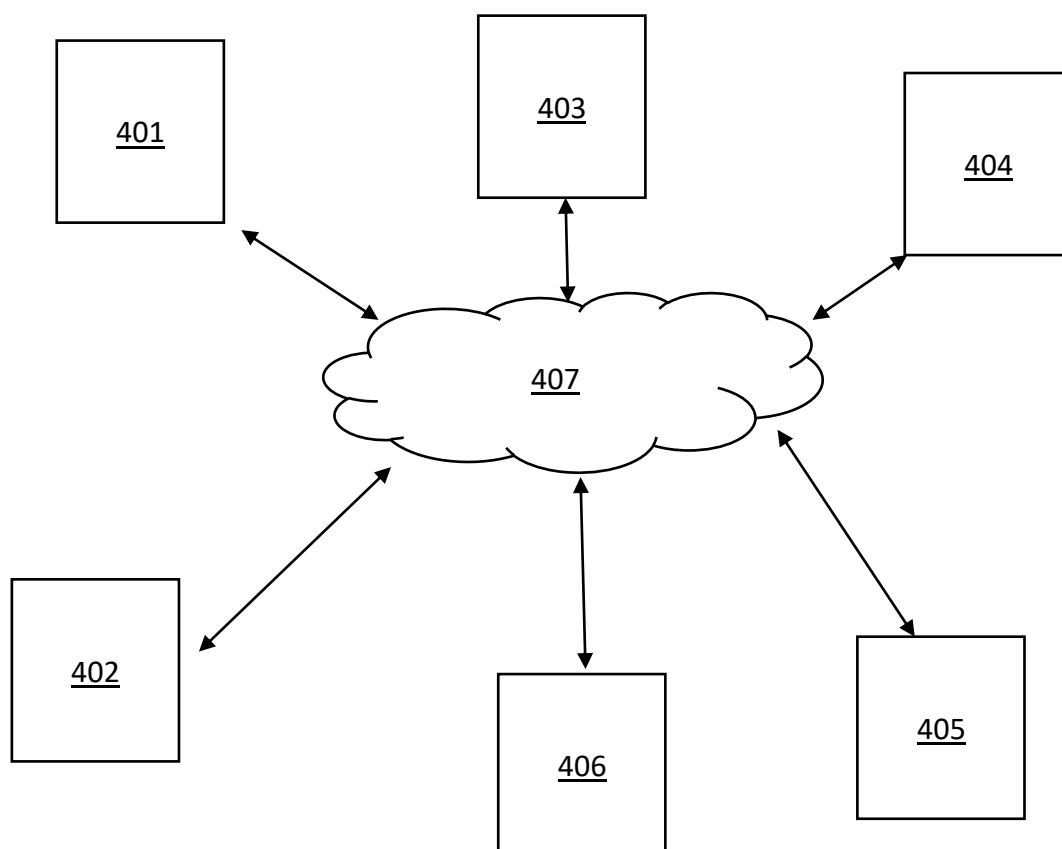


Fig. 14