

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;

 comparar, por medio de la interfaz del dispositivo móvil, la selfie con la fotografía del ees la misma persona y evitar que una tercera persona firme a nombre del usuario;

25 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;

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

35 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;

5

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

10

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

15

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 ser servidor una copia de la constancia de certificación en una base de datos;

20

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.

25

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.

30

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.

35

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.
- 5
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:
- 10
- notificar a un usuario que tiene un documento, que, al ser aceptado, se le debe incorporar una firma autógrafa digital;
- 15
- escanear, un documento de identificación del usuario que va a firmar;
- determinar, si la información que fue escaneada es correcta;
- 20
- 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;
- 25
- 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;
- enviar a un servidor de la institución emisora del documento de identificación, los datos recabados para validar la información proporcionada por el usuario;
- 30
- obtener, el documento a firmar, activando a su vez una herramienta para videgrabar el trazo de la firma del usuario sobre la pantalla del dispositivo móvil, así como una videgrabación con la lectura del texto en donde se compromete a cumplir el acuerdo que se está adquiriendo;
- 35

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;

el servidor Back-end FAD se configura para:

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;

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;

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;

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

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.

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.

- 5 **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.
- 10 **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:
- 15 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;
- determinar si la información que fue escaneada es correcta;
- 20 obtener, por medio de la interfaz del dispositivo móvil, la huella dactilar del usuario que va a firmar;
- tomar una selfie del usuario que va a firmar, esto como un comprobante de vida;
- 25 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;
- 30 enviar a un servidor de la institución emisora del documento de identificación, los datos recabados para validar la información proporcionada por el usuario;
- 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
- 35 como una videograbación con la lectura del texto en donde se compromete a cumplir el acuerdo que se está adquiriendo;

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

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

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

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

15 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 servidor una copia de la constancia de certificación en una base de datos;

20 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;

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