(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 934 075**

(51) Int. CI.:

***G06F 21/64*** (2013.01)
***G06Q 20/38*** (2012.01)
***H04L 9/32*** (2006.01)
***H04W 12/08*** (2011.01)
***G06Q 20/02*** (2012.01)
***G07F 17/40*** (2006.01)
***H04W 12/084*** (2011.01)
***H04L 9/08*** (2006.01)
***H04L 9/14*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.10.2020 E 20204182 (8)**

(97) Fecha y número de publicación de la concesión europea: **14.09.2022 EP 3812945**

(54) Título: **Sistema abierto y seguro para el procesamiento de la solicitud de firma electrónica y método asociado**

(30) Prioridad:

**27.10.2019 FR 1912020**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**16.02.2023**

(73) Titular/es:

**LEX PERSONA (100.0%)**
**2, rue Gustave Eiffel**
**10430 Rosières-près-Troyes, FR**

(72) Inventor/es:

**DEVORET, FRANÇOIS;**
**SCHWEBLIN, BENOIT y**
**PASQUIER, JULIEN**

(74) Agente/Representante:

**MARTÍN SANTOS, Victoria Sofia**

## DESCRIPCIÓN

Sistema abierto y seguro para el procesamiento de la solicitud de firma electrónica y método asociado

Ámbito de la técnica

La invención se relaciona con el campo de la firma electrónica. Más particularmente, la invención se refiere a un sistema abierto y seguro para procesar solicitudes de firma de documentos electrónicos. La invención se refiere además a un método para generar y procesar una solicitud de firma.

Técnica anterior

La firma electrónica consiste principalmente en permitir a una persona humana usuaria encriptar una huella digital de un documento a firmar, con una clave privada correspondiente a una clave pública asociada a su identidad, estando esta clave privada generalmente protegida por un dispositivo criptográfico y un código secreto, debiendo entonces incorporarse o asociarse el resultado de la encriptación al documento a firmar para que constituya prueba. Durante esta operación, es necesario asegurarse de que la asociación entre la clave pública y la identidad del firmante esté certificada por una autoridad compatible con los requisitos de seguridad y confianza asociados a la firma electrónica, que esta certificación sea verificada como aún válida, y que el firmante está de acuerdo con el contenido a firmar.

Además, la secuencia de tareas de cálculo, gestión y verificación necesarias para producir una firma electrónica es excesivamente compleja. De hecho, los algoritmos en los que se basan los cálculos deben ser compatibles con los requisitos de seguridad y confianza. Además, los datos a firmar no necesariamente son directamente accesibles por el proceso de firma, pero pueden ser remotos, y estos mismos datos a firmar deben poder enmarcarse en elementos contextuales como la fecha y hora de la firma, el nombre del firmante, la cadena de certificación, rol, lugar de firma, política de firma, etc. Además, la clave privada puede estar en un dispositivo criptográfico local o distante del usuario, y el entorno mismo de estas operaciones a veces está en la estación de trabajo del usuario, pero también puede ser remoto o ejecutarse en modo cliente-servidor en un explorador de Internet, o en un teléfono inteligente o tableta.

El documento EP 1393144 B1 da a conocer un método y un sistema basados en la red [web] para la firma legalmente exigible de documentos en un entorno basado en la red. El sistema incluye un primer medio de acceso para acceder al entorno web desde un sistema electrónico, e incluye también una pluralidad de módulos. Un módulo de representación de documentos para presentar al usuario una representación web del documento, un módulo de información legal para presentar al usuario, en el entorno web, información legal relacionada con la firma electrónica del documento, y para obtener el consentimiento del usuario a este información legal. Un módulo de aprobación de documentos para integrar la firma del usuario al documento, con el consentimiento del usuario de la información legal. El sistema también incluye un módulo de registro para generar un registro de proceso de la firma del documento asociando este registro de proceso con el documento firmado. Finalmente, un módulo de distribución de documentos para poner a disposición el documento firmado. Este documento se refiere a la trazabilidad del proceso. Existe una necesidad particular de agilizar el proceso de firma electrónica y también ocultar la complejidad del proceso a los usuarios.

El documento EP 3423982 A1 (del solicitante Lex Persona) divulga un sistema de firma electrónica abierto y seguro que comprende una solicitud comercial que solicita la firma de un documento de un administrador de firma para un usuario. La solicitud comercial define las especificaciones de las firmas, por ejemplo el contenido a firmar, la selección de un usuario firmante, de un formato de firma, etc. El gestor de firma coordina la solicitud de firma y actúa como intermediario entre la solicitud comercial y el usuario mediante la verificación de la autorización de la solicitud comercial, la identidad del usuario firmante; recupera el documento a firmar, prepara la solicitud de firma con los cálculos dactiloscópicos de los datos a firmar, y envía una notificación de la solicitud de firma a los servicios de firma del usuario. El usuario, a través de los servicios de firma, puede controlar la ejecución del proceso de firma mediante la activación de la clave privada correspondiente a un certificado del usuario que cumple los criterios de selección enviados al gestor de firma por la solicitud comercial con objeto de cifrar la huella dactilar de los datos a firmar. En este documento, el proceso de firma electrónica se desglosa en tareas independientes cuyas interacciones entre ellas son seguras. Este documento muestra una agilización del proceso de firma electrónica y oculta la complejidad a los usuarios de la firma electrónica y a las aplicaciones empresariales que deseen implementarla.

El propósito de la presente invención es permitir la creación sobre la marcha de un certificado de firma en la propia estación de trabajo del firmante y firmar un documento. La presente invención simplifica considerablemente el problema de la firma remota y en particular la obligación de demostrar el control de la clave privada por parte de su titular, pero también el problema de asegurar esta clave privada gestionada centralmente o bien la confidencialidad de la información firmada.

Otro objeto de la invención es mejorar el nivel de seguridad de la transacción de la firma y permitir una identidad sustancial o reforzada pero también la generación de un identificador de la transacción de la firma que permita generar sobre la marcha una identidad digital específicamente creado para una transacción en particular.

Sumario de la invención

El objetivo de la presente invención es simplificar el problema de firmar electrónicamente un documento de forma remota, asegurar la gestión de las claves privadas y también mejorar aún más el nivel de seguridad así como la confidencialidad de la información que se firma. Para ello, se propone un sistema abierto y seguro para la tramitación de solicitudes de firma electrónica de documentos, compuesto por una solicitud comercial, encargada de generar una solicitud de firma de al menos un documento para un usuario firmante, siendo alojada dicha solicitud comercial por una entidad solicitante, el sistema se caracteriza porque permite firmar documentos con un certificado de servidor creado sobre la marcha y porque además comprende tres servicios independientes, un servicio de administración de solicitudes que aloja las solicitudes de firma y los documentos adjuntos; una página de consentimiento, que consta de una aplicación HTML, que puede gestionar el protocolo de consentimiento interactuando con un servicio seguro de identificación de usuarios y que genera un par de claves de cliente, KcliPub y KcliPriv, en el explorador de Internet del firmante, y un servicio de gestión de pruebas, alojado por un proveedor de firma, que recoge las pruebas de firma y que comprende un componente de servidor que aloja la clave criptográfica del firmante, siendo dicho servicio de gestión de pruebas capaz de recuperar un certificado de una autoridad de certificación, para generar un par de claves de servidor, KservPub, KservPriv para derivar una clave secreta Ks utilizando la clave pública del cliente y la clave privada del servidor, y para generar una clave pública KPub y una clave privada (KPriv) del firmante, siendo utilizada la clave secreta Ks para empaquetar la clave privada del firmante.

Según características particulares, el servicio de gestión de solicitudes está protegido por una clave API de tal forma que sólo la aplicación de negocio es capaz de hacerle peticiones de firma y pudiendo dicho servicio de gestión de solicitudes generar una solicitud de petición de firma, entonces generar un identificador aleatorio único para uno o más documentos de la solicitud de firma y calcular el hash *[huella digital, resumen digital, o conjunto de datos que tienen un tamaño o longitud fija, acerca del contenido de un documento]* de dichos documentos, calcular el hash de dicha solicitud de firma, crear un token [clave, prueba o registro] de la solicitud, con una duración limitada, para usar una frase de contraseña, compartido con el controlador de pruebas, para firmar dicho token de solicitud, luego cambiar el estado de la solicitud de firma a "iniciado" y devolver el token firmado de la solicitud a la solicitud comercial.

Según características particulares, la página de consentimiento se genera en el navegador del usuario, a pedido de la solicitud comercial que transmite el token de solicitud a través del servicio de solicitud de firma, dicha página de consentimiento genera un par de claves de cliente (kcliPriv y kcliPub) luego interactúa con el servicio de identificación del usuario, a través de una nueva pestaña en el navegador, una vez que el usuario es autenticado por el proveedor de identidad, este último transmite un código al usuario, el gestor de pruebas luego le pide al proveedor de identidad un token de identificación a cambio del código, según el protocolo OpenId Connect.

Según características particulares, la página de consentimiento es servida por el servicio de gestión de pruebas, de manera que el gestor de pruebas devuelve la cadena de certificados y la clave pública del servidor, a saber, KservPub, a la página de consentimiento, dicha página de consentimiento utilizando la clave privada del cliente (Kclipriv) y la clave pública del servidor (KservPub) es capaz de derivar la clave secreta Ks, siendo el firmante el único que dispone de dicha clave secreta Ks, necesaria para descomponer su clave privada, Kpriv, a través de dicha página de consentimiento que se ejecuta en su explorador de Internet .

De acuerdo con características particulares, el administrador de prueba puede validar el token de solicitud, generar una identificación de prueba y crear un archivo de prueba, la identificación de prueba se deriva del token de solicitud de tal manera que la evidencia de creación no se puede reproducir.

Según características particulares, el servicio de identificación con el que interactúa la página de consentimiento es tal que permite obtener una identidad sustancial o reforzada del usuario y crear un certificado cualificado.

Según características particulares, la página de consentimiento es capaz de recuperar la solicitud de firma y la lista de documentos a firmar del gestión de solicitudes, presentando la página de consentimiento los documentos al firmante, permitiéndole leerlos antes de firmarlos.

Según características particulares, el gestor de solicitudes es capaz de generar el valor de los documentos a firmar, DTBS, y enviar a la página de consentimiento adjuntando un código de autenticación, HMAC, dicha página de consentimiento es capaz de enviar el HMAC y la clave secreta Ks, y que siendo el gestor de pruebas capaz de validar los HMAC y descomprimir la clave privada KPriv del firmante utilizando la clave secreta Ks, dicho gestor de pruebas firma entonces los valores DTBS, con la clave privada KPriv del firmante y añade los valores DTBS y la firma al expediente de prueba.

Según características particulares, el archivo de pruebas se exporta en formato XML, dicho archivo se firma mediante un certificado de seguridad y se envía a la página de consentimiento que lo traslada al gestor de solicitudes para la validación y almacenamiento de dicho archivo de pruebas.

Según características particulares, el gestor de solicitudes, después de haber recibido el archivo de pruebas en formato XML, es capaz de producir los documentos firmados de forma asíncrona e informar a la solicitud comercial de estos documentos, pudiendo la solicitud comercial recuperar los documentos firmados y el fichero XML de evidencia utilizando una clave API, después de haber archivado el fichero XML y los documentos firmados, pudiendo la solicitud comercial transmitir los documentos firmados al firmante.

Según características particulares, el sistema también comprende una aplicación nativa que accede a la clave criptográfica del firmante, pudiendo ejecutarse dicha aplicación nativa en el ordenador del firmante o en su teléfono inteligente, y permitiendo a dicho firmante firmar documentos con su propio certificado utilizando bien su ordenador o una aplicación móvil si desea firmar en su teléfono inteligente.

Según características particulares, la página de consentimiento después de haber recuperado los documentos a firmar en la gestión de solicitudes y después de haber obtenido el consentimiento del firmante puede abrir la aplicación nativa ya sea en el ordenador o en el teléfono inteligente del firmante, la aplicación nativa puede solicitar al firmante que elija un certificado de firma, recuperar el DTBS de los documentos a firmar en la gestión de solicitudes, enviar el DTBS firmado al gestor de pruebas, solicitar la producción del archivo de pruebas y transferir el archivo de pruebas al gestión de solicitudes para generar los documentos firmados de forma asíncrona.

1. La invención también se refiere a un método para elaborar y procesar una solicitud de firma implementado en el sistema anterior, que comprende una solicitud comercial para realizar una solicitud de firma, un servicio de gestión de solicitudes que tiene en cuenta la solicitud de firma de la solicitud comercial, una página de consentimiento para gestionar el protocolo de consentimiento, y un servicio de gestión de pruebas para la generación y actualización de un expediente de pruebas, caracterizándose el método por permitir la firma de uno o varios documentos con un certificado de servidor y por incluir las siguientes etapas:

- poner en marcha de la solicitud comercial de un usuario para firmar un documento;
- lanzar la solicitud de firma por parte de la solicitud comercial al gestión de solicitudes, luego transfiere los documentos a firmar y el usuario es redirigido a la página de consentimiento;
- identificar al firmante mediante la página de consentimiento con el proveedor de identidad a través del protocolo OpenID Connect;
- recuperar la solicitud de firma y los documentos a firmar a través de la página de consentimiento del administrador de la solicitud;
- solicitar el consentimiento para que los documentos sean firmados por la página de consentimiento del firmante;
- generar la clave de firma en el componente servidor del gestor de pruebas,
- recuperar la DTBS del (de los) documento(s) a firmar con la gestión de solicitudes a través de la página de consentimiento;
- solicitar la firma de DTBS para los documentos del servidor y la producción de un archivo de pruebas con el gestor de pruebas a través de la página de consentimiento;
- transferir el archivo de pruebas al gestor de solicitudes para generar los documentos firmados de forma asíncrona;
- redirigir el firmante a la gestión de solicitudes;
- enviar los documentos firmados y el archivo de pruebas a la solicitud comercial;
- archivo de los documentos firmados y el archivo de pruebas por la solicitud comercial.

2. El método comprende además las siguientes etapas:

- solicitar la validación del token, la generación de una identificación de prueba y la creación de un archivo de pruebas por parte del gestor de pruebas;
- generar un par de claves de cliente KcliPriv, Kclipub mediante la página de consentimiento;
- crear la clave del firmante por parte del gestor de pruebas;
- generar un par de claves privadas y públicas del servidor y el uso de la clave privada del servidor y la clave pública del cliente para derivar una clave secreta Ks que empaqueta la clave privada del firmante, por el gestor de pruebas;
- solicitar el certificado a la autoridad de certificación y devolver la cadena de certificados y la clave pública del servidor a la página de consentimiento del gestor de pruebas;
- generar los valores DTBS de la solicitud y los documentos por parte del gestión de solicitudes;
- transmitir de los valores DTBS a través de la página de consentimiento (43) al gestor de pruebas;
- firmar los valores DTBS con la clave privada del firmante y adición de los valores DTBS y la firma al archivo de prueba;
- exportar el archivo de pruebas en formato XML y lo envía de vuelta a la página de consentimiento que luego lo envía al gestión de solicitudes;
- producir documentos firmados y enviar dichos documentos a la solicitud comercial;
- archivar el archivo de pruebas en formato XML y los documentos firmados por la solicitud comercial y luego la transferencia de los documentos firmados al firmante.

3. La invención también se relaciona con el método para desarrollar y procesar una solicitud de firma implementado en el sistema anterior, y que comprende además una aplicación nativa que accede a una clave criptográfica del firmante. El proceso, después de recuperar los documentos a firmar de la gestión de solicitudes y después de haber obtenido el consentimiento del firmante, comprende las siguientes etapas:

- abrir la aplicación nativa en el ordenador del firmante o en su teléfono inteligente;
- solicitar de elección de un certificado de firma por parte de la aplicación nativa;
- recuperar el DTBS de los documentos a firmar en el gestor de solicitudes, luego enviar el DTBS firmado al gestor de pruebas por la aplicación nativa;
- solicitar la producción del archivo de pruebas, y transferirlo del archivo de pruebas a la gestión de solicitudes para generar los documentos firmados de forma asíncrona;
- cerrar la aplicación nativa y redireccionar el firmante a la solicitud comercial;
- recuperar los documentos firmados mediante la solicitud comercial;
- recuperar el expediente de prueba y archivar los expedientes así como de los documentos firmados por la solicitud comercial.

Breve descripción de los dibujos

Otras características, detalles y ventajas de la invención se harán evidentes con la lectura de la siguiente descripción, con referencia a las figuras adjuntas, que ilustran:

La figura 1 ilustra la arquitectura general del sistema según la presente invención.

La figura 2 representa un diagrama simplificado del servidor de firma con un certificado creado sobre la marcha según la presente invención.

La figura 3 ilustra la arquitectura del sistema en el caso de uso de un token de autenticación y firma local.

La figura 4 representa un esquema simplificado en el caso de firma local.

Para mayor claridad, los elementos idénticos o similares se identifican con idénticas referencias en todas las figuras.

Descripción de las realizaciones

La arquitectura general del sistema según la presente invención representa, por un lado, un usuario 30 que debe firmar un documento y, por otro lado, el entorno de internet de un gestor de solicitudes de firma. Un usuario 30 es una persona física que desea o debe firmar uno o más documentos.

La distinción entre una firma realizada por iniciativa propia del usuario o solicitada por un tercero (otro usuario) es fundamental. En efecto, la experiencia del usuario es muy diferente porque, en el primer caso, se trata necesariamente de una preparación vinculada a la elección del documento, su redacción, la elección de la identidad digital y su implementación, la posible política de firma a aplicar, etc., mientras que en el segundo caso exige una especial facilidad de actuación en cuanto al acceso al documento y a la identidad digital del firmante para centrarse en el valor probatorio de la transacción, obligando eventualmente al usuario, antes de poder firmar, a leer todo el documento, autenticarse para acreditar su identidad digital, etc.

La arquitectura del sistema como se representa en la figura 1 comprende una solicitud comercial 10, dicha solicitud comercial 10 puede ser desarrollada y ejecutada en diversos entornos tales como servidores de red, navegadores de Internet, en un entorno PC o Mac nativo, o nuevamente desde un teléfono móvil o tableta. La solicitud comercial está en el origen del proceso de firma, por lo que cualquier solicitud de firma, ya sea que se realice por iniciativa del propio usuario firmante 30, o que se realice por un tercero para que se firme un documento, necesariamente debe pasar por esta solicitud comercial 10. Dicha solicitud comercial 10 está diseñada para que sea capaz de realizar una solicitud de firma de al menos un documento desde un servicio de gestión de solicitudes 41, dicho gestor de solicitudes 41 es un componente servidor que tiene en cuenta una solicitud de firma procedente de dicha solicitud comercial 10 y está alojada en una entidad solicitante 40.El sistema también comprende otros dos servicios independientes, a saber, un servicio de gestión o una página de consentimiento 43 y un servicio de gestión de pruebas 45.

La página de consentimiento 43 gestiona el protocolo de consentimiento y es una aplicación HTML que conduce al firmante 30 a través del proceso de consentimiento y a la creación de la firma. Este componente reside en el navegador de Internet 11 del firmante 30. El servicio de gestión de pruebas 45 es un componente servidor que recoge las pruebas, este componente está alojado en el proveedor de firmas 50 (LEXPERSONA). La referencia 48 es un componente de servidor que aloja la clave criptográfica del firmante 30. Este componente está integrado en el gestor de pruebas 45. La autoridad de certificación 46 es una infraestructura de clave pública PKI que emite el certificado del firmante, este componente está alojado por el proveedor de firmas 50. El proveedor de identidad 44

es un servidor de autorización compatible con Open ID Connect que emite un token de identificación de firmante del que se deriva el certificado de firmante. Este componente está alojado por un proveedor de registros 60.

La figura 2 ilustra el diagrama simplificado del proceso de firma remota de documentos. El firmante 30 navega con su navegador de Internet 11 en la solicitud comercial 10 donde debe firmar ciertos documentos. La solicitud comercial 10 lanza una solicitud de firma en la gestión de solicitudes 41 y le transfiere los documentos a firmar. El servicio de gestión de solicitudes 41 redirige al firmante 30 a la página de consentimiento 43. Dicha página de consentimiento 43 identifica al firmante 30 interactuando con un proveedor de identidad 44 usando el protocolo Open ID Connect. Entonces, la página de consentimiento 43 recupera la solicitud de firma así como los documentos a firmar en la gestión de solicitudes 41. La página de consentimiento 43 muestra los documentos a firmar al firmante 30 pidiéndole su consentimiento.

La página de consentimiento solicita la generación de la clave de firmante en el componente del servidor 48 que está integrado con el componente del gestor de pruebas 45.La página de consentimiento 43 recupera el DTBS de los documentos a firmar en la gestión de solicitudes 41 y solicita al servidor 48 que firme el DTBS y el gestor de pruebas 45 para producir el archivo de pruebas, para transferir al gestión de solicitudes 41 para que dicho gestión de solicitudes 41 pueda generar los documentos firmados de forma asíncrona. Luego, la página de consentimiento 43 redirige al firmante a la solicitud comercial 10. Una vez que la gestión de solicitudes 41 ha producido los documentos firmados, la solicitud comercial 10 los recupera. La solicitud comercial 10 también recupera el archivo de pruebas y lo archiva con los documentos firmados.

A continuación se describirá cómo una solicitud comercial 10 proporciona una solicitud de firma en la gestión de solicitudes 41. De hecho, la solicitud comercial 10 inicia la creación de una solicitud de firma con la gestión de solicitudes 41 que está protegida por una clave API. La solicitud comercial 10 es la única aplicación capaz de realizar una solicitud de firma a la gestión de solicitudes 41. Cabe señalar que la solicitud comercial 10 se comunica con la API REST de la gestión de solicitudes 41 en segundo plano para que la clave API permanezca secreta. La gestión de solicitudes 41 luego genera una ID de solicitud de firma y la envía a la solicitud comercial 10, dicha solicitud comercial 10 descarga un documento para que sea firmado en la gestión de solicitudes 41 al pasar la ID de solicitud como parámetro. De manera similar, la administración de solicitudes 41 genera una ID de documento única y la devuelve a la solicitud comercial 10. Las etapas anteriores se repiten tantas veces como documentos haya que firmar. Una vez descargados los documentos, la solicitud comercial 10 solicita al gestor de solicitudes 41 que inicie la solicitud de firma.

La gestión de solicitudes 41 calcula el hash de la solicitud así como los hash del documento a partir del JSON (del inglés "Java Script Object Notation") de la solicitud y los JSON del documento (incluidos los hash del documento). El JSON de solicitud que incluye un ID de solicitud. La gestión de solicitudes 41 también crea la solicitud de token que contiene la ID de solicitud y su hash y usa una frase de contraseña compartida con el gestor de pruebas 45 para firmarlo. Posteriormente, la gestión de solicitudes 41 cambia el estado de la solicitud a iniciada y devuelve el token de solicitud a la solicitud comercial 10. El token de solicitud tiene una vida útil de cinco minutos. Una duración más corta causaría problemas si los relojes de la gestión de solicitudes 41 y el gestor de pruebas 45 no están correctamente sincronizados.

Creación de una página de consentimiento:

El firmante es redirigido a la URL de la página de consentimiento 43 por la solicitud comercial 10, pasando el token de solicitud como parámetro. El gestor de pruebas 45, detrás de la URL 43 de la página de consentimiento, valida el token de solicitud, genera una identificación de prueba y crea el archivo de pruebas, devolviendo una redirección HTTP con la identificación de prueba como parámetro. La identificación de prueba se deriva del token de solicitud para que la creación de evidencia [o pruebas] no se pueda reproducir. Esto se debe a que la redirección evita el intento de crear evidencia cada vez que el firmante actualiza la pestaña de su navegador. A continuación, el firmante abre la URL 43 de la página de consentimiento y pasa la identificación de prueba como parámetro. El gestor de pruebas 45 envía de vuelta una página HTML que incluye la identificación de la solicitud, hash de solicitud, URL de autorización del proveedor de identidad 44, hojas de estilo, etc. a la página de consentimiento 43. Recuperación de la identidad del firmante y procedimiento de autorización Open ID Connect:

Una vez servida la página de consentimiento 43, el firmante 30 la carga en su navegador 11. En primer lugar, la página de consentimiento genera un par de claves pública y privada del cliente (KcliPriv y KcliPub). Luego, la URL autorizada se completa con un estado que contiene la identificación de prueba, un identificador aleatorio único para uno o más documentos y la clave pública del cliente. Se realizará una redirección al proveedor de identidad 44 a través de un botón presentado al firmante 30. El botón también permite que se abra la página de autorización sin ninguna restricción del navegador. Una vez que se hace clic en el botón, la URL de autorización del proveedor de identidad 44 se abre en una nueva pestaña del navegador 11, dejando la página de consentimiento 43 en segundo plano. Mantener abierta la página de consentimiento 43 permite mantener la clave privada del cliente (KcliPriv) en RAM y limitar el riesgo de ataque al ordenador del firmante 30. Una vez que el firmante 30 se ha autenticado y ha otorgado autorización para acceder a su identidad, el proveedor de identidad 44 lo redirige a una página de recordatorio transmitiéndole un código.

El navegador del firmante 30 abre la página de devolución de llamada pasando la identificación de prueba como un parámetro con el código. El gestor de pruebas 45 solicita al proveedor de identidad 44 que intercambie el código con un token de identificación según lo especificado por el protocolo Open ID Connect. El proveedor de identidad 44 devuelve el token de identificación al gestor de pruebas 45. Dicho gestor de pruebas 45 crea el token de firmante a partir del token de ID y actualiza el archivo de pruebas y se devuelve una página HTML, que incluye el token de firmante. Téngase en cuenta que el token del firmante contiene el hash de la solicitud y ciertos elementos básicos proporcionados por el proveedor de identidad 44, como el nombre del firmante, la dirección de correo electrónico y el identificador. Una vez abierta por el navegador del firmante 11, la página de devolución de llamada envía el token del firmante a la página de consentimiento 43, usando un mensaje entre pestañas. Dado que ambas páginas están en el mismo dominio, no hay restricciones de navegador.

Consentimiento del firmante:

La página de consentimiento 43 recupera la solicitud de firma de la gestión de solicitudes 41 pasando la identificación de la solicitud y el token de firmante como parámetro. La gestión de solicitudes 41 devuelve el JSON de la solicitud después de verificar que el token de firmante contiene los elementos de identidad esperados, así como el hash de solicitud esperado. La página de consentimiento 43 recupera la lista de documentos de la gestión de solicitudes 41 pasando la identificación de la solicitud y el token del firmante como parámetro. La gestión de solicitudes 41 devuelve el JSON de los documentos después de verificar que el token de firma contiene los elementos de identidad y el hash de solicitud previsto. La página de consentimiento 43 garantiza que el hash de la solicitud sea coherente con el JSON de la solicitud y los JSON del documento. Para cada documento que el firmante debe o desea leer o descargar, la página de consentimiento 43 recupera el contenido del documento pasando como parámetros la identidad del documento y el token del firmante. La gestión de solicitudes 41 devuelve el contenido del documento después de verificar que el token de firmante contiene los elementos de identidad esperados y el hash de solicitud esperado. Antes de presentar el contenido del documento al firmante, la página de consentimiento 43 garantiza que el hash del contenido es consistente con el hash contenido en el documento JSON. A continuación, la página de consentimiento 43 presenta los documentos al firmante 30, permitiéndole leerlos. Una vez que acepta, el firmante hace clic en el botón “acepto”.

Creación de la clave del firmante:

La clave del firmante es creada y protegida por el gestor de pruebas 45. De hecho, la página de consentimiento 43 le pide al gestor de pruebas 45 que cree la clave de firmante 30, pasando la identificación de prueba, el token de firmante, la solicitud JSON, el documento JSON y la clave pública de cliente (kcliPub) como parámetros. El gestor de pruebas 45 asegura que el hash de la solicitud sea consistente con el JSON de la solicitud y con el JSON de los documentos. El gestor de pruebas 45 también verifica que el número aleatorio único contenido en el token de identificación producido por el proveedor de identidad 44 coincida con el hash de desafío y la clave pública de cliente (kcliPub).

A continuación, el gestor de pruebas 45 genera un par de claves de servidor (kservPriv y kservPub) y utiliza la clave privada del servidor (kservPriv) y la clave pública del cliente (kcliPub) para derivar una clave secreta (Ks) con el algoritmo Diffie-Hellman. A continuación, el gestor de pruebas 45 crea el par de claves del firmante (kPriv y kPub) con una solicitud de certificado, y la clave secreta (Ks) se usa para empaquetar la clave privada del firmante (kPriv). Una vez que se ha empaquetado la clave del firmante, el gestor de pruebas 45 destruye la clave secreta (Ks). La solicitud de certificado se envía a la autoridad de certificación 46. La autoridad de certificación 46 devuelve el certificado al gestor de pruebas 45.

Después de almacenar el encapsulado clave privada y actualizando el archivo de pruebas con el certificado del firmante, el gestor de pruebas 45 devuelve la cadena de certificados y la clave pública del servidor (kservPub) a la página de consentimiento 43. La página de consentimiento 43 utiliza la clave privada del cliente (kcliPriv) y la clave pública del servidor (kservPub) para derivar la clave secreta (Ks) con el algoritmo Diffie-Hellman. En este punto, el firmante 30, a través de la página de consentimiento 43 que se ejecuta en su propio navegador 11, es el único que tiene la clave secreta (Ks) necesaria para descomprimir la clave privada del firmante (kPriv) en el gestor de pruebas.

A continuación se describe cómo la gestión de solicitudes 41 genera los documentos DTBS y cómo los firma el manejador de evidencia 45 usando la clave de firmante 30. De hecho, para cada documento que se firma, la página de consentimiento 43 envía la cadena de certificados a la gestión de solicitudes 41 con el identificador del documento y el token del firmante. Después de verificar que el token del firmante contiene los elementos de identidad esperados y el hash de la solicitud, la gestión de solicitudes 41 genera el valor DTBS y lo devuelve a la página de consentimiento 43 adjuntando un HMAC.

El HMAC se calcula a partir del valor DTBS y el ID del documento utilizando la frase de contraseña compartida con el gestor de pruebas 45. Una vez que se han generado todos los valores DTBS, la página de consentimiento 43 se envía al gestor de pruebas 45 con los HMAC y la clave secreta (Ks). El gestor de pruebas 45 valida los HMAC y desempaqueta la clave privada del firmante (kPriv) con la clave secreta (Ks). Luego, el gestor de pruebas 45 firma

los valores DTBS con la clave privada del firmante (kPriv) y agrega los valores DTBS y la firma al archivo de pruebas. El archivo de pruebas se exporta en formato XML, lo firma el gestor de pruebas 45 con un certificado de sellado y se devuelve a la página de consentimiento 43. Dicha página de consentimiento 43 transmite el archivo de pruebas XML a la gestión de solicitudes 41. La gestión de solicitudes 41 valida y almacena el archivo de pruebas XML, cambia el estado de la solicitud a 'firmado' y devuelve una respuesta vacía a la página de consentimiento 43.

El gestión de solicitudes 41 completa el procesamiento de la solicitud produciendo los documentos firmados en segundo plano. De hecho, después de haber recibido el archivo de pruebas XML, la gestión de solicitudes 41 inicia una tarea en segundo plano para producir los documentos firmados y completar el procesamiento de la solicitud. Mientras tanto, la página de consentimiento 43 redirige al firmante 30 a la URL de devolución de llamada de la solicitud comercial 10. El navegador del firmante 30 abre la página de devolución de llamada de la solicitud comercial 10. Según el caso de uso de la solicitud comercial 10, la página de recordatorio puede solicitar el firmante 30 esperar mientras se preparan los documentos firmados o puede informarle que los documentos firmados estarán disponibles más tarde. Una vez que la gestión de solicitudes 41 produce los documentos firmados, el estado de la solicitud cambia a completo.

La gestión de solicitudes 41 informa a la solicitud comercial 10 a través de un Webhook. La solicitud comercial 10 recupera los documentos firmados de la gestión de solicitudes 41 usando su clave API. La gestión de solicitudes 41 devuelve el archivo de pruebas XML a la solicitud comercial 10. Una vez que se han archivado el archivo de pruebas XML y los documentos firmados, la solicitud comercial 10 transmite los documentos firmados al firmante 30.

Téngase en cuenta que un Webhook es un método para aumentar o modificar el comportamiento de una página web, o una aplicación red, con devoluciones de llamada personalizadas.

La invención también permite que un firmante firme documentos con su propio certificado, un token criptográfico, por ejemplo, utilizando una aplicación local si desea firmar en su ordenador o si desea usar su teléfono inteligente. Los diversos componentes que intervienen en la creación de la firma local se ilustran en la figura 3. Esta arquitectura comprende una solicitud comercial 10 que se encarga de crear las solicitudes de firma. Este componente está alojado por la entidad solicitante 40. La gestión de solicitudes 41 es un componente del servidor que aloja las solicitudes de firma y los documentos adjuntos. Este componente está alojado por la entidad solicitante 40. La página de consentimiento 43 es una aplicación HTML que dirige al signatario 30 a lo largo del proceso de consentimiento y la creación de la firma. Este componente reside en el explorador de Internet 11 del firmante 30. El gestor de pruebas 45 es un componente de servidor que recopila la evidencia de la firma. Este componente está alojado en el proveedor de firmas 50 (LEX PERSONA). El sistema comprende además una aplicación nativa local 47 que se puede instalar en un ordenador de sobremesa de la oficina o en un smartphone y que accede a la clave criptográfica del firmante para firmar los documentos. Este componente se ejecuta en el ordenador o teléfono inteligente del firmante.

La figura 4 que ilustra un flujo simplificado de este modo de firma local. En este modo de firma local, una vez que la página de consentimiento 43 muestra los documentos al firmante 30 y solicita su consentimiento, dicha página de consentimiento 43 abre la aplicación de escritorio/móvil local, dicha aplicación de escritorio/móvil local 47 le pide al firmante 30 que elija un certificado de firma. La aplicación de escritorio/móvil local recupera el DTBS de los documentos a firmar del gestión de solicitudes 41 y luego envía el DTBS firmado al gestor de pruebas 45 y le pide que produzca el archivo de pruebas. El archivo de pruebas se transfiere a la gestión de solicitudes 41 para generar los documentos firmados de manera asíncrona. A continuación, la página de consentimiento 43 redirige al firmante 30 a la solicitud comercial 10. El firmante accede a la solicitud comercial 10, y una vez que la gestión de solicitudes 41 ha producido los documentos firmados, la solicitud comercial 10 los recupera. La solicitud comercial 10 recupera el archivo de pruebas y lo archiva con los documentos firmados. Apertura de la aplicación local de escritorio/móvil:

El firmante 30 pasa de la página de consentimiento 43 a la aplicación local de escritorio/móvil 47 para firmar con su token criptográfico. En este modo de firma local, la página de consentimiento 43 solicita al firmante 30 que instale la aplicación local 47 en su escritorio o en su teléfono inteligente o que la abra si la aplicación ya está instalada transmitiendo como parámetros la identificación de solicitud, identificación de prueba, y una identificación de instancia aleatoria. Si se abre la Página de consentimiento 43 en un explorador de Internet de escritorio, el firmante puede cambiar a la aplicación móvil en su teléfono inteligente usando un código QR. De lo contrario, la aplicación móvil/de escritorio local se abre a través de una URL personalizada. Una vez abierta, la aplicación de escritorio/móvil local llama a la gestión de solicitudes 41 para establecer la identificación de instancia correspondiente a la identificación de solicitud especificada. El propósito es que la página de consentimiento 43 sea notificada cuando se haya abierto la aplicación local de escritorio/móvil 47. La gestión de solicitudes 41 devuelve el JSON de la solicitud. La aplicación de escritorio/móvil local recupera la lista de documentos de la gestión de solicitudes 41 pasando la identificación de la solicitud como un parámetro. La gestión de solicitudes 41 devuelve el JSON de los documentos. Se solicita al firmante 30 que elija un certificado de firma y luego el firmante hace clic en el botón "firmar".

En este modo de firma local, el gestor de pruebas 45 devuelve la cadena de certificados a la aplicación de escritorio/móvil local. Para cada documento a firmar, la aplicación local de escritorio/móvil envía la cadena de certificados al administración de solicitudes 41 con la identificación del documento. La gestión de solicitudes 41

genera el valor DTBS y lo envía de vuelta a la página de consentimiento 43. Una vez que se han generado todos los valores DTBS, la aplicación móvil/de escritorio local los firma con la clave de firma y los envía al gestor de pruebas 45 con los HMAC y los valores de firma.

El gestor de pruebas 45 valida los HMAC y los valores de firma, luego agrega los valores de DTBS y firma al archivo de pruebas. El archivo de pruebas se exporta en formato XML, se firma mediante el gestor de pruebas 45 con un certificado de sellado y se devuelve a la aplicación móvil/de escritorio local. La página de consentimiento 43 pasa el archivo de pruebas XML a la gestión de solicitudes 41. La gestión de solicitudes 41 valida y almacena el archivo de pruebas, cambia el estado de la solicitud a firmado y devuelve una respuesta vacía a la página de consentimiento 43. A continuación, la aplicación móvil/de escritorio local se cierra y devuelve el firmante 30 a la página de consentimiento 43.

**REIVINDICACIONES**

1. Sistema abierto y seguro de tramitación de solicitudes de firma electrónica de documentos que comprende

- una solicitud comercial (10), encargada de generar una solicitud de firma de al menos un documento para un usuario firmante (30), la solicitud comercial (10) está alojada en una entidad solicitante (40), el sistema se caracteriza por que permite firmar documentos con un certificado de servidor creado sobre la marcha y también porque comprende un servicio de gestión de solicitudes (41) que aloja solicitudes de firma y documentos adjuntos;

- una página de consentimiento (43), generada en el navegador del usuario a petición de la solicitud comercial (10); y,

- un servicio de gestión de pruebas (45), alojado por un proveedor de firmas (50), que recopila las pruebas de firmas;

la página de consentimiento (43) que consiste en una aplicación HTML, al interactuar con un servicio de identificación seguro (44) del usuario (30), a través de una nueva pestaña en el navegador, genera un par de claves de cliente, Kclipub, KcliPriv, una vez que el usuario es autenticado por el proveedor de identidad (44) según el protocolo Openld Connect, y cuando se obtiene un token de identificación a petición del gestor de pruebas (45) del proveedor de identidad (44) a cambio de un código enviado por dicho proveedor de identidad (44) al usuario (30), el gestor de pruebas (45) puede validar el token de identificación, para generar una identificación de prueba y crear un archivo de prueba, derivándose la identificación de prueba del token de identificación de tal manera que la creación de prueba o evidencia no puede ser reproducida;

el servicio de gestión de pruebas (45) comprende además un componente de servidor que aloja la clave criptográfica del firmante (30), y que puede generar un par de claves de servidor, KservPriv y KservPub, para derivar una clave secreta Ks utilizando la clave pública del cliente, Kclipub y la clave privada del servidor, KservPriv, para generar una clave pública KPub y una clave privada, KPriv del firmante (30), para crear una solicitud de certificado, para recuperar un certificado de una autoridad de certificación (46);

en donde la clave secreta Ks se utiliza para empaquetar la clave privada del firmante devolviendo la cadena de certificados y la clave pública del servidor, KservPub a la página de consentimiento (43), utilizando dicha página de consentimiento la clave privada del cliente Kclipriv, y la clave pública del servidor, KservPub es capaz de derivar la clave secreta Ks, y que el firmante (30) es el único que tiene dicha clave secreta Ks, necesaria para desglosar su clave privada Kpriv a través de dicha página de consentimiento (43) que se ejecuta en su explorador de Internet, el controlador de pruebas (45) puede usar la clave privada, KPriv del firmante, descomprimida con la clave secreta Ks y generada con el controlador de solicitudes (41), para firmar el valor DTBS y agregar el los valores DTBS y la firma del archivo de prueba evidencia para crear una evidencia de firma para ser almacenada;

la gestión de solicitudes (41), después de haber recibido el archivo de prueba en formato XML, puede producir los documentos firmados e informar a la solicitud comercial (10) de estos documentos, la solicitud comercial (10) puede recuperar los documentos firmados y el archivo de prueba XML utilizando una clave API, y después de haber archivado el archivo XML y los documentos firmados, la solicitud comercial (10) es capaz de transmitir los documentos firmados al firmante (30).

2. Sistema abierto y seguro para el procesamiento de solicitudes de firma electrónica de documentos según la reivindicación 1, caracterizado por que el servicio de gestión de solicitudes (41) está protegido por una clave API para que solo la solicitud comercial (10) pueda realizarle solicitudes de firma y por que el servicio de gestión de solicitudes (41) puede generar una solicitud para la solicitud de firma, luego generar un identificador aleatorio único para uno o más documentos de la solicitud de firma y calcular el hash de dichos documentos, calcular el hash de dicha solicitud para la solicitud de firma, creando un token de la solicitud, con una duración limitada, utilizando una frase secreta, compartida con el gestor de pruebas (45), para firmar dicho token de solicitud, luego cambiar el estado de la solicitud de firma a "iniciada" y devolver el token de solicitud firmado a la solicitud comercial (10).

3. Sistema abierto y seguro para el procesamiento de solicitudes de firma electrónica de documentos según la reivindicación 1, caracterizado por que el servicio de identificación (44) con el que interactúa la página de consentimiento (43) es tal que permite obtener una identidad sustancial o reforzada del usuario (30) y crear un certificado cualificado.

4. Sistema abierto y seguro para el procesamiento de solicitudes de firma electrónica de documentos según una de las reivindicaciones anteriores, caracterizado en que la página de consentimiento (43) puede recuperar la solicitud de firma y la lista de documentos a firmar de la gestión de solicitudes (41), presentando la página de consentimiento los documentos al firmante (30), permitiéndole leerlos antes de firmarlos.

5. Sistema abierto y seguro para la tramitación de solicitudes de firma electrónica de documentos según la reivindicación 1 en el que el archivo de pruebas se exporta en formato XML, siendo firmado dicho archivo por un certificado de seguridad y enviado a la página de consentimiento (43) que lo traslada a la gestión de solicitudes (41) de validación y almacenamiento del expediente de pruebas.

6. Sistema abierto y seguro para el procesamiento de solicitudes de firma electrónica de documentos según la reivindicación 1, caracterizado por que el sistema comprende además una aplicación nativa (47) que accede a la clave criptográfica del firmante (30), dicha aplicación nativa (47) que puede ejecutarse tanto en el ordenador del firmante (30) como en su teléfono inteligente, y que permite a dicho firmante (30 ) para firmar documentos con su propio certificado usando su ordenador o una aplicación móvil que quiera firmar en su teléfono inteligente.

7. Sistema abierto y seguro para el procesamiento de solicitudes de firma electrónica de documentos según la reivindicación 1, caracterizado por que, la página de consentimiento (43) después de haber recuperado los documentos a firmar en la gestión de solicitudes (41) y después de haber obtenido el consentimiento del firmante (30) puede abrir la aplicación nativa (47) en el ordenador de escritorio o en el teléfono inteligente del firmante (30), la aplicación nativa (47) puede solicitar al firmante (30) que elija un certificado de firma, recuperar el DTBS de los documentos a firmar en el gestor documental (41), enviar el DTBS firmado al gestor de pruebas (45), para solicitar la producción del archivo de pruebas y transferir el archivo de pruebas a la gestión de solicitudes (41) para generar los documentos firmados de forma asincrónica.

8. Proceso de generación y tramitación de solicitudes de firma implementado en el sistema de las reivindicaciones 1 a 7, caracterizado por que comprende las siguientes etapas:

- solicitar validación de token, generar una identificación de prueba y crear un archivo de pruebas por parte del gestor de pruebas (45), alojado por un proveedor de firma (50), recopilando la evidencia de firma;

- generar un par de claves de cliente KcliPriv, Kclipub por la página de consentimiento (43), consistiendo dicha página de consentimiento (43) en una aplicación HTML interactuando con un servicio de identificación segura (30) a través de una nueva pestaña en el navegador y generada en el navegador del usuario a petición de la solicitud comercial (45), una vez que el usuario es autenticado por el proveedor de identidad (44) según el protocolo OpenId Connect y cuando se obtiene el token de identificación a petición del gestor de pruebas (45), del proveedor de identidad (44) a cambio de un código enviado por dicho proveedor de identidad (44) del usuario (30) al usuario (30), el gestor de pruebas (45) valida el token de identificación, genera una identificación de prueba y crea un archivo de pruebas, derivándose la identificación de prueba del token de identificación de manera que la creación de evidencia no se puede reproducir;

- crear la clave pública KPub y la clave privada KPriv del firmante (30) mediante el gestor de pruebas (45);

- generar por parte del gestor de pruebas (45) de un par de claves privadas y públicas del servidor, KservPriv y KservPub, y el uso de la clave privada del servidor, KservPriv y la clave pública del cliente, KcliPub para derivar una clave secreta Ks, necesaria para descomponer la clave privada KPriv del firmante (30) a través de la página de consentimiento (43), el administrador de prueba (45) usa la clave privada KPriv del firmante usando la clave secreta Ks que empaqueta la clave privada del firmante (30);

- solicitar certificado a la autoridad de certificación y devolver la cadena de certificados y la clave pública del servidor, KservPub, a la página de consentimiento (43) mediante el gestor de pruebas (45);

- generar los valores DTBS de la solicitud y los documentos por parte de la gestión de solicitudes (41);

- transmitir los valores DTBS a través de la página de consentimiento (43) al gestor de pruebas (45);

- firmar los valores DTBS con la clave privada KPriv del firmante (30) y añadir los valores DTBS y la firma al archivo de pruebas;

- exportar el archivo de pruebas en formato XML y regresar a la página de consentimiento (43) que luego lo transmite a la gestión de solicitudes (41);

- producir documentos firmados y enviar dichos documentos a la solicitud comercial (10);

- archivar el archivo de pruebas en formato XML y los documentos firmados por la solicitud comercial (10) y luego transferir los documentos firmados al firmante (30).

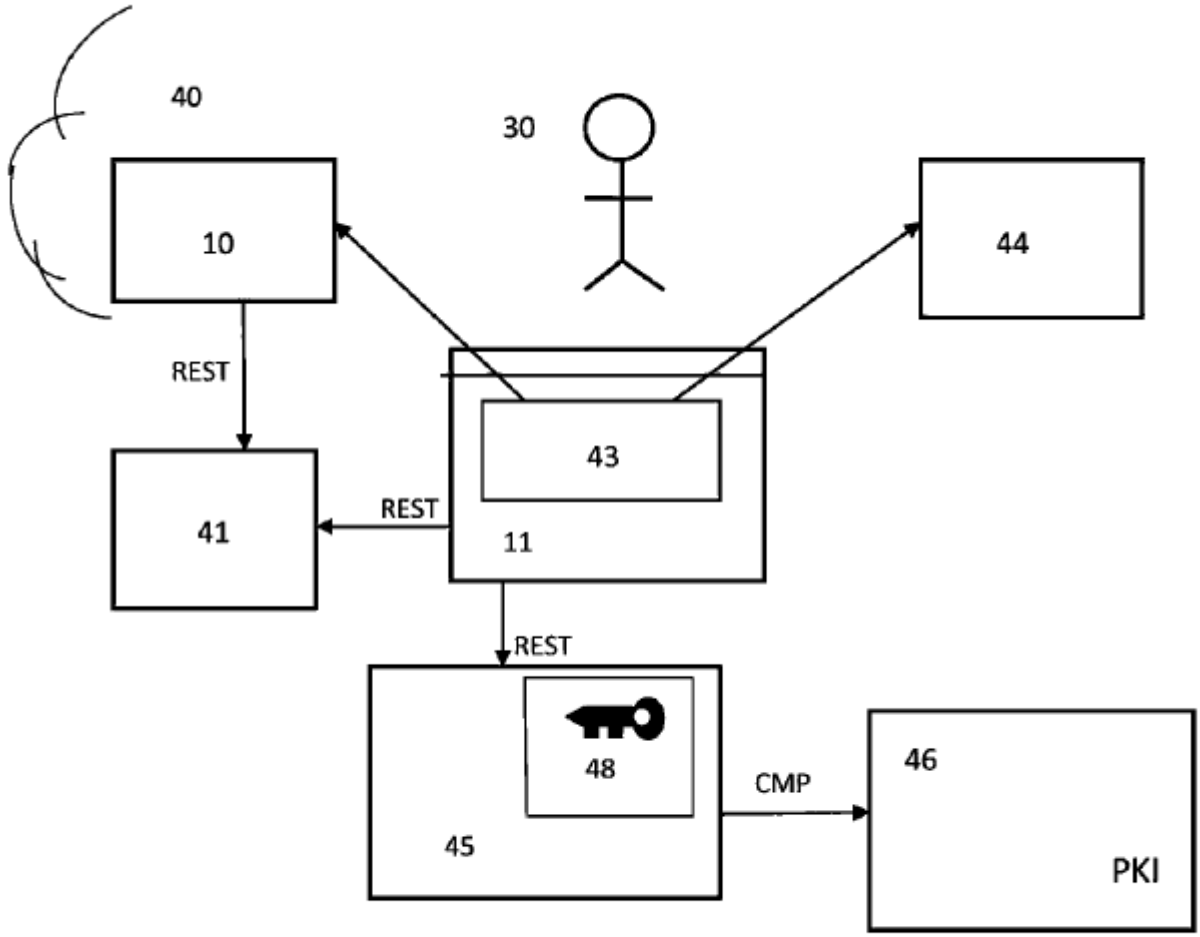


FIG.1

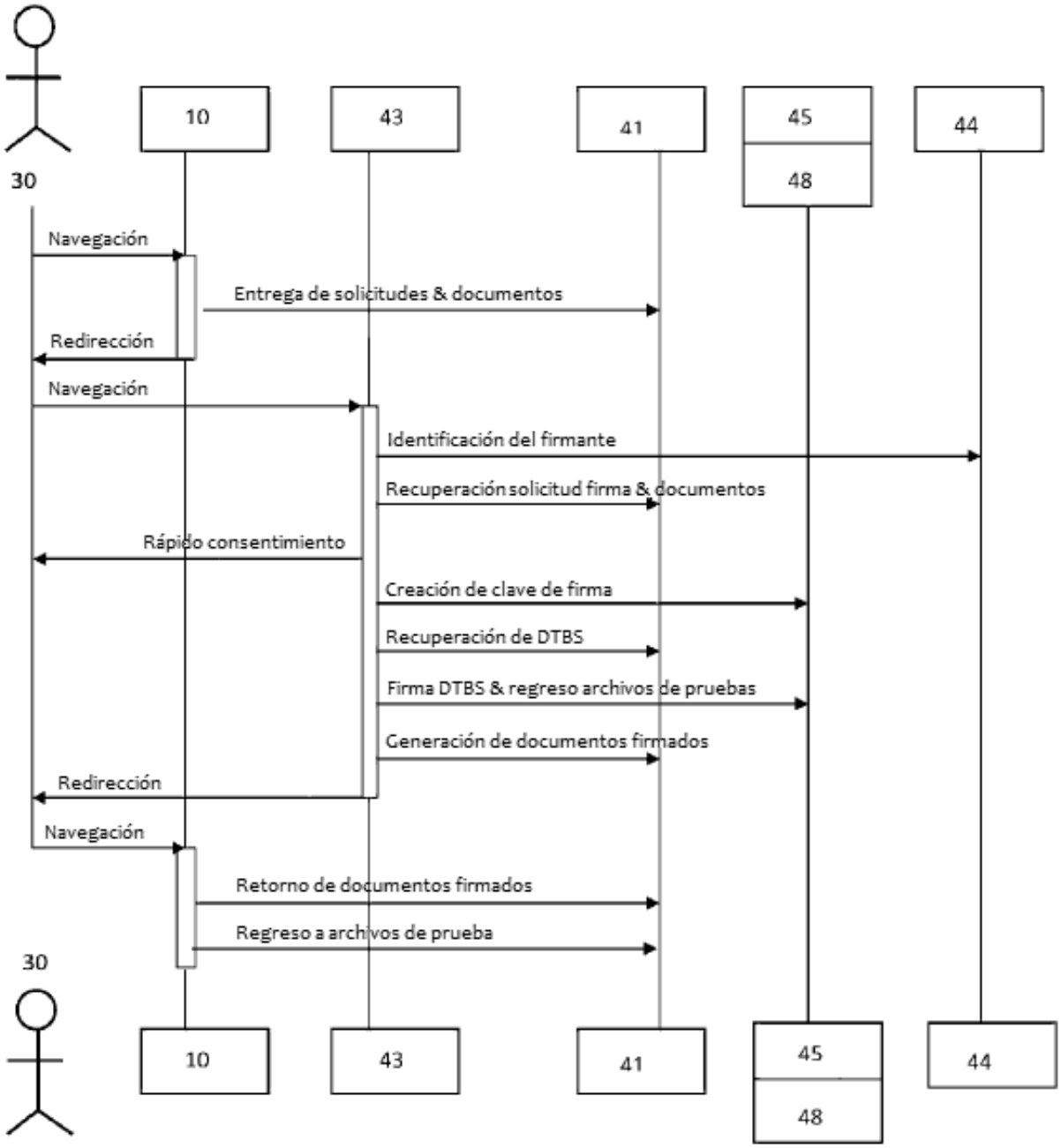
30
10
43
41
45
48
44
Navegación
Entrega de solicitudes & documentos
Redirección
Navegación
Identificación del firmante
Recuperación solicitud firma & documentos
Rápido consentimiento
Creación de clave de firma
Recuperación de DTBS
Firma DTBS & regreso archivos de pruebas
Generación de documentos firmados
Redirección
Navegación
Retorno de documentos firmados
Regreso a archivos de prueba
30
10
43
41
45
48
44

FIG.2

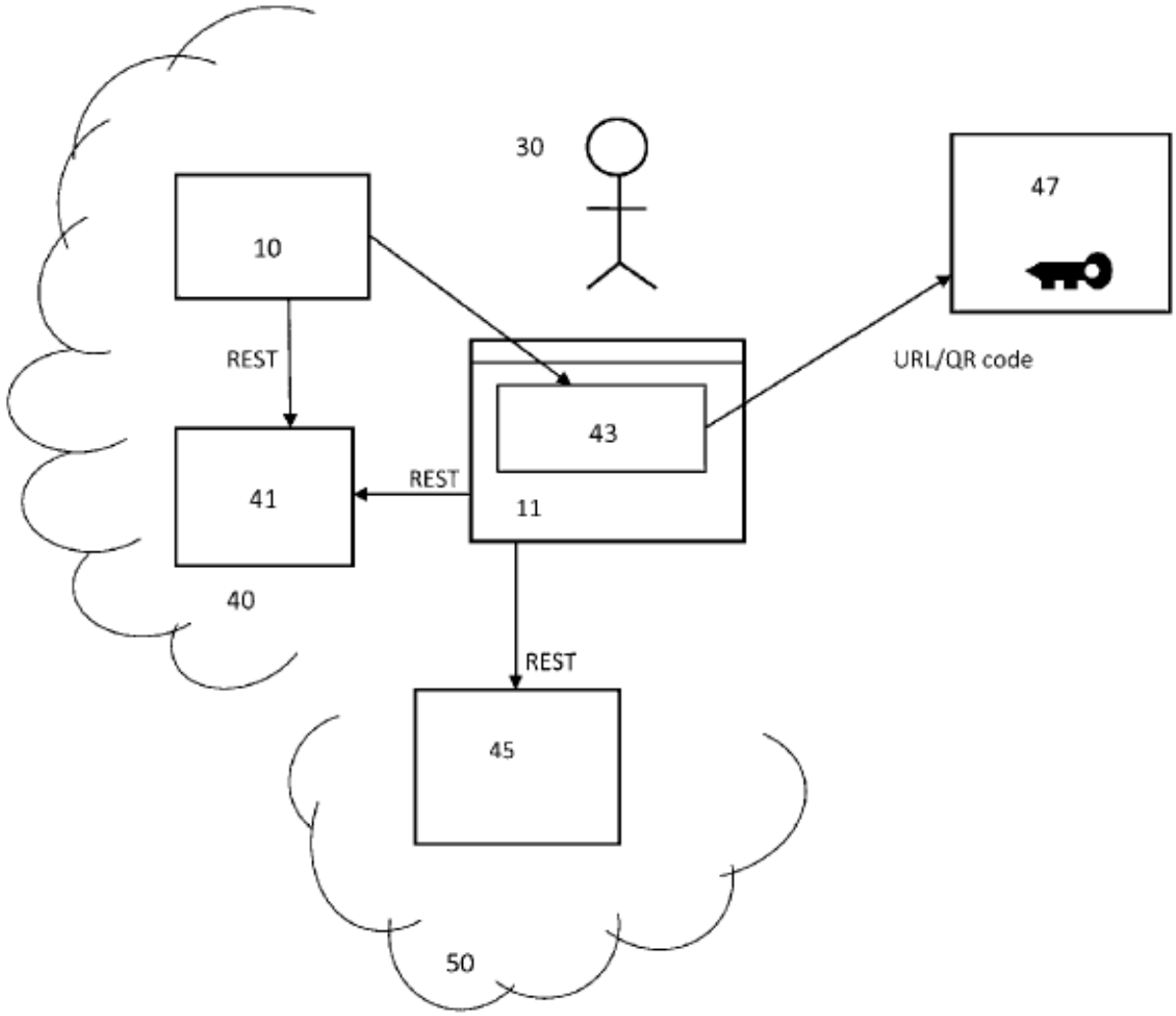


FIG.3

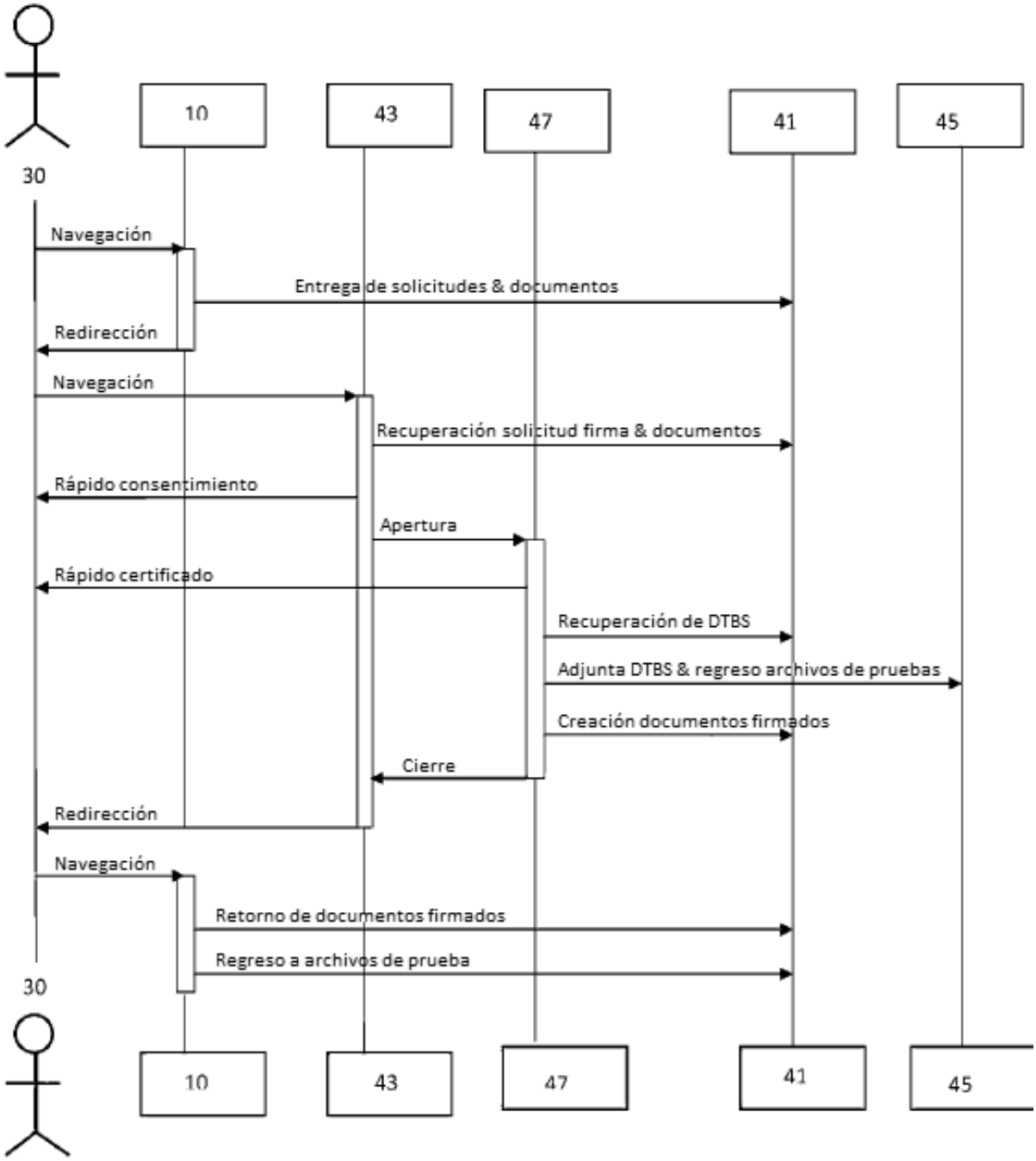
30
10
43
47
41
45
Navegación
Entrega de solicitudes & documentos
Redirección
Navegación
Recuperación solicitud firma & documentos
Rápido consentimiento
Apertura
Rápido certificado
Recuperación de DTBS
Adjunta DTBS & regreso archivos de pruebas
Creación documentos firmados
Cierre
Redirección
Navegación
Retorno de documentos firmados
Regreso a archivos de prueba
30
10
43
47
41
45

FIG.4