(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 748 942**

(51) Int. CI.:

G06F 21/64 (2013.01)
G06F 21/60 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.09.2013 E 13186755 (8)**

(97) Fecha y número de publicación de la concesión europea: **22.05.2019 EP 2717191**

(54) Título: **Método para crear una firma digital**

(30) Prioridad:

02.10.2012 IT MI20121639

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2020

(73) Titular/es:

BIT4ID S.R.L. (100.0%)
Via Diocleziano, 107
80125 Napoli, IT

(72) Inventor/es:

PALAZZO, VINCENZO

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Método para crear una firma digital

Campo técnico

La presente invención se refiere a un método para crear una firma digital. En particular, la presente invención se refiere a dicho método anterior en donde un firmante de un documento formateado digital aplica una clave criptográfica propia en un método de firma digital, cuya correcta ejecución se determina mediante al menos otro parámetro, tal como por ejemplo un algoritmo criptográfico seleccionado para el método de firma.

En particular, la presente invención se refiere a definir un esquema para facilitar el proceso de firma digital de un documento.

Técnica conocida

Como es sabido, con el fin de crear una firma digital en un documento electrónico, se prevé insertar una clave criptográfica de un firmante de una solicitud de firma que recibe el documento electrónico de entrada a ser firmado.

En particular, con el fin de aplicar una firma digital en el documento electrónico, es necesario dotar a la solicitud de firma con un certificado de firma que esté asociado al firmante y aplicar la clave criptográfica (clave privada) por medio de un dispositivo seguro, tal como una tarjeta inteligente.

Un certificado digital es un documento electrónico que atestigua la asociación única entre la clave pública y la identidad de un sujeto (persona, empresa, ordenador, etc.) que declara su uso en el ámbito de procedimientos de cifrado asimétrico y/o autenticación por medio de una firma digital. Tal certificado se proporciona por un tercero, que es de confianza y reconocido como autoridad de certificación (CA), que a su vez se autentifica con el fin de evitar falsificación a través de firma digital o se cifra por la clave privada de la asociación, que entonces proporciona la clave pública asociada respectiva con propósitos de verificación.

Una firma digital es por ejemplo un paso necesario para proporcionar un servicio a una dirección de internet, a la que también se proporciona el documento a ser firmado. El servicio y el documento a ser firmado se almacenan, por ejemplo, en un servidor en red, tal como sobre Internet, al que se puede acceder con un dispositivo electrónico perteneciente al firmante, por ejemplo, un dispositivo de mano, un ordenador personal y similares, que también están conectados a la red y están dotados con un navegador, para acceder a direcciones de Internet.

En otras palabras, se requiere la provisión de una firma digital con el fin de acceder a un servicio proporcionado a través de Internet y para el cual se ha de presentar un documento electrónico firmado. En tal escenario, el servicio se proporciona por un servidor web, en el que se almacena el documento a ser firmado.

En métodos conocidos, para una aplicación adecuada de una firma digital, no es suficiente que el firmante aplique su clave criptográfica sino que es necesario que ejecute correctamente algunas operaciones tales como descargar el documento a ser firmado y asociado al servicio requerido, seleccionar un algoritmo para firmar, al que aplicar la clave de firma, e insertar una o más informaciones que se requieran generalmente al firmante y que pueden incluir, por ejemplo, teclear un código de comprobación del firmante o enviar un acuse de recibo para el tratamiento de datos, sin el cual el proceso de firma no se puede aceptar o completar correctamente.

Sustancialmente, para aplicar correctamente la firma digital es necesario que el usuario tenga información auxiliar adicional, que cualifique la operación, por ejemplo puede ser necesario conocer el tipo de certificado a ser usado (por ejemplo un certificado de autenticación, un certificado de suscripción) o el algoritmo de firma a ser usado. Con el fin de usar el servicio web también se requiere a menudo conocer el formato de archivo a ser usado para firmar (por ejemplo un pdf firmado) y la forma de enviarlo al proveedor (por ejemplo entrega de correo a través de POST de http).

Tales operaciones, que se han de realizar por el firmante, hacen que el método de firma digital llegue a ser propenso a errores, dificultando su adecuada difusión.

Tomemos por ejemplo el siguiente caso:

Un usuario abre el navegador en su dispositivo electrónico, por ejemplo, un ordenador personal o portátil, y accede a un servicio a través de una dirección de Internet, con el fin de descargar un documento a ser compilado y firmado, guardándolo, por ejemplo, en un directorio en el dispositivo, en un formato de archivo doc, pdf, docx o txt. El usuario puede recibir el documento a ser compilado y firmado por correo electrónico, y entonces guardarlo, como se ha dicho anteriormente.

No obstante, en ambos casos, el usuario puede modificar la extensión del archivo a ser firmado, por ejemplo de .doc a .pdf, no permitiendo, por lo tanto, que el método de firma digital proceda correctamente.

Además, si el dispositivo digital es un dispositivo móvil, por ejemplo, uno con un sistema operativo iOS o Android, se

ha de dotar con una aplicación que reciba el documento a ser firmado desde el navegador, dado que en tales sistemas no existe ninguna disposición para un guardado preliminar en carpetas de documentos. En este caso, el usuario tiene que determinar si su dispositivo electrónico está dotado o no con una aplicación que pueda leer el documento a ser firmado, y, si es necesario, identificar e instalar esta aplicación en el dispositivo.

En cualquier caso, para firmar el documento, el usuario no solamente ha de usar la aplicación de firma requerida, sino que también ha de seleccionar que uno o más parámetros sean introducidos en la aplicación de firma, además de su clave criptográfica. Es obvio que pueden ocurrir errores durante estos procedimientos.

Por ejemplo, suponiendo que el documento a ser firmado es un archivo pdf, la aplicación de firma se puede establecer en un formato “por defecto” de aplicación de firma, por ejemplo, el formato CAdES (Firmas Electrónicas Avanzadas CMS), que genera un archivo firmado que tiene una extensión .p7m. No obstante, se puede requerir, para una correcta ejecución del servicio requerido, aplicar un algoritmo diferente para el formato de firma, tal como el formato PAdES (Firmas Electrónicas Avanzadas PDF); por lo tanto, si el usuario no modifica la configuración “por defecto” para la aplicación de firma, la firma digital es incorrecta, aunque se proporcione una clave criptográfica válida.

Obviamente, entre diferentes escenarios de error, hay uno en el que el usuario/firmante aplica una clave adecuada, aunque no la que se requiere realmente, por ejemplo, puede introducir erróneamente una clave de autenticación en lugar de una clave de suscripción.

Por lo tanto los errores pueden multiplicarse: el usuario adquiere el archivo a ser firmado de la entidad solicitante, descargándolo a través de su propio navegador de Internet o recibiéndolo como un archivo adjunto a un mensaje de correo que se envía automáticamente. El archivo tiene una extensión clásica como .pdf, .doc, .docx, .txt, con un software asociado instalado en el sistema anfitrión, permitiendo su procesamiento.

A través de reconocimiento de la extensión de archivo, el tipo MIME, el sistema anfitrión del usuario iniciará la ejecución de la aplicación requerida con el fin de mostrar su contenido. En sistemas de sobremesa, el navegador permite guardar archivos a través de aplicaciones web en el sistema de archivos, dentro de un directorio elegido por el usuario (por ejemplo, Escritorio, o Descarga). Una vez el archivo se ha recibido, el usuario puede interactuar con él fácilmente, por ejemplo, haciendo doble clic puede iniciar la aplicación de software permitiéndolo ser mostrado o editado. A partir de entonces, el archivo descargado se puede enviar a la aplicación de firma digital, usando el procedimiento correspondiente, tal como arrastrando el icono del archivo por encima del icono de la aplicación de firma. En sistemas móviles que usan plataformas populares tales como iOS y Android, el archivo se envía directamente desde el navegador a una aplicación de software instalada que se ha registrado para ese tipo de extensión de archivo/MIME particular. La aplicación de firma se ha de registrar, por lo tanto, como una aplicación compatible adicional para el tipo de archivo proporcionado por la aplicación web.

El usuario firma el documento usando un cliente de firma conforme a las regulaciones válidas y se envían normalmente instrucciones adicionales con respecto a los parámetros de configuración a ser usados al usuario de la aplicación web por un mensaje de voz.

Una vez que se ha aplicado la firma, el usuario transmite el documento firmado al organismo solicitante a través de un canal proporcionado por este último, por ejemplo, por correo electrónico o a través de carga usando una aplicación web. Normalmente, el documento firmado digitalmente es un archivo que tiene una extensión .p7m o .pdf (archivos pdf firmados digitalmente en su formato nativo tienen la misma extensión que archivos pdf sin firma digital). En sistemas móviles, el archivo firmado digitalmente siempre se posee por la aplicación de firma digital, que ha de tener algún tipo de mecanismo de transmisión autónomo que sea compatible con el proporcionado por la aplicación web o que al menos tenga que proporcionar un modo de transmisión de archivos firmados a otra aplicación, que entonces puede proceder con su transmisión.

El escenario propuesto muestra que, con el fin de aplicar una firma a un documento, el usuario no solamente tiene que usar la aplicación de firma apropiada, sino también los parámetros correctos para ejecutar el procedimiento, y está claro que durante estas operaciones pueden ocurrir algunos errores.

Por ejemplo, supongamos que el documento a ser firmado es un archivo pdf. En este caso, la aplicación de firma se puede configurar en un modo “por defecto” para aplicar un cierto formato de firma, tal como CAdES (Firmas Electrónicas Avanzadas CMS), que genera un archivo firmado que tiene una extensión .p7m. No obstante, para una correcta ejecución del servicio, se puede requerir aplicar un formato de firma diferente, tal como PAdES (Firmas Electrónicas Avanzadas PDF); por lo tanto, si el usuario no modifica la configuración “por defecto” para la aplicación de firma, la firma digital es incorrecta, pese a ejecutar un proceso de firma formalmente correcto. Otro error probable que el usuario se puede encontrar es el uso de un certificado que no es válido para una operación de firma, en donde el usuario/firmante puede usar, por ejemplo, un certificado de autenticación en lugar de un certificado de suscripción.

También se conocen métodos para firmar digitalmente un documento, que guían al usuario a través del uso de “objetos web activos” tales como controles ActiveX o miniaplicaciones Java. Los controles ActiveX son, por ejemplo, una tecnología desarrollada por Microsoft® para extender las funciones de una aplicación, por ejemplo, el

navegador, añadiendo nuevos comandos.

De manera similar, las miniaplicaciones son programas escritos en lenguaje Java, que se puede ejecutar por un navegador web. Se usan miniaplicaciones para crear páginas web dotadas con funciones interactivas, tales como guiar al usuario a través de los pasos de firma.

El uso de “objetos web activos” también presenta algunos problemas con respecto a la tecnología usada, tales como la provisión de los mismos objetos para diferentes plataformas, es decir, diferentes sistemas operativos. Varias soluciones que se usan actualmente no proporcionan interoperabilidad entre:

- sistemas operativos,

- navegadores,

- tecnologías para proteger las claves de firma digital asimétricas (por ejemplo del tipo de firma remota de tarjeta inteligente).

Otro problema intrínseco a la adopción de “objetos web activos” es el hecho de que se usan a menudo para ciberataques. Finalmente, existe también la limitación debido al hecho de que no se pueden usar en un entorno móvil, dado que los navegadores web para dispositivos móviles, que están basados en iOS y Android, no permiten su uso.

El documento US 2003/093678 presenta un método para crear una firma digital; la solicitud de firma se envía desde un dispositivo de cliente a un servidor, en el que el cliente se debe autenticar; la firma se ejecuta en el servidor, después de la autenticación del cliente.

El objeto técnico de la presente invención es por lo tanto proporcionar un método para firma digital automática, que evita errores en la firma, simplificando el proceso requerido y proporcionando lo mismo para todos los usuarios y todos los dispositivos electrónicos, superando, por lo tanto, las limitaciones que aún afectan a los métodos de la técnica conocida.

Compendio de la invención

La presente invención se resuelve en base al concepto de incorporar toda información necesaria para ejecutar correctamente una firma digital dentro de un archivo formateado, que se introduce a una aplicación de firma de un dispositivo electrónico de usuario o firmante, que es capaz de extraer la información y recibir además una clave criptográfica del firmante, con el fin de ejecutar el método de firma digital.

En particular, la aplicación de firma se almacena y ejecuta en un dispositivo electrónico de usuario o firmante, por ejemplo, un teléfono inteligente o dispositivo de mano o en un ordenador personal que también almacena la clave criptográfica para su firma.

El documento a ser firmado se envía, por ejemplo, por un servidor remoto, así como el archivo formateado que contiene la información o los parámetros para su firma.

En una realización modificada, la clave criptográfica no se almacena físicamente en el dispositivo electrónico de usuario sino que se transmite, sin embargo, al dispositivo electrónico de usuario, por ejemplo por medio de una tarjeta inteligente o una tarjeta SIM como para ser conectadas al dispositivo electrónico, y que almacena la clave criptográfica. En otras palabras, la clave criptográfica y la firma o autenticación no se almacenan remotamente sino que están presentes en el dispositivo electrónico de usuario. Más en particular, la firma del documento a ser firmado se ejecuta físicamente en el dispositivo electrónico, pero los parámetros de la firma se envían desde un servidor remoto al dispositivo electrónico y se incorporan en el archivo formateado.

Ventajosamente, según la solución, se eliminan esencialmente posibles errores durante el método de firma, dado que solamente se requiere que el firmante introduzca su clave criptográfica en la aplicación de firma, por ejemplo, seleccionándola con su dispositivo electrónico, y dado que toda la otra información requerida para ejecutar el método se incorpora en el archivo formateado. Ventajosamente, tal archivo formateado también puede estar compuesto del archivo a ser firmado.

La ventaja de tal método es evidente cuando un servicio, por ejemplo, un servicio proporcionado por un servidor en una dirección de Internet determinada, se lleva a cabo solamente siguiendo una firma digital específica, es decir, una firma que requiere parámetros específicos.

De hecho, al contrario de los métodos conocidos, el servicio no envía el documento a ser firmado al firmante, sino que en su lugar lo dota con el archivo formateado que incorpora tanto la información o parámetros requeridos para la firma digital, como el documento a ser firmado. Cuando el dispositivo electrónico del firmante recibe el archivo formateado, automáticamente ejecuta la aplicación de firma, extrayendo el documento a ser firmado y la información para su correcta firma digital del archivo formateado, por ejemplo, un algoritmo criptográfico específico a ser usado.

El firmante está libre de cualquier control o acción requerida por el método de firma, y ventajosamente puede concentrarse en leer el documento a ser firmado y en la inserción o selección de su correcta clave criptográfica, para su firma.

En otras palabras, la solución inventiva consiste en: crear una estructura de datos que incorpora el documento a ser firmado y toda la información requerida para una correcta aplicación de la firma digital, según las especificaciones establecidas por la solicitud de firma.

La aplicación de firma, al recibir dicha entrada de estructura de datos anterior, ejecuta autónomamente y correctamente el método de firma. La probabilidad de error en estos procedimientos de firma es igual a cero, y solamente se requiere al usuario que permita el uso de su clave criptográfica por dicha aplicación de firma, que poseerá toda la información requerida para ejecutar el método.

La ventaja proporcionada por tal método es evidente en todas aquellas situaciones en las que con el fin de obtener un servicio, se requiere aplicar una firma que tiene propiedades específicas en un archivo que se descarga de un servidor web. Según la presente invención, el usuario no descarga el archivo a ser firmado y lo firma con los métodos usuales, sino que en su lugar descarga un archivo que contiene dicha estructura de datos anterior, que también incluye el documento a ser firmado junto a toda la información requerida para aplicar la firma y transmitirla sucesivamente a un organismo solicitante.

Cuando el dispositivo electrónico del firmante recibe el archivo que contiene la estructura de datos incluida en el archivo formateado, ejecuta automáticamente la aplicación de firma, extrayendo de él el documento a ser firmando y la información para una correcta firma digital, por ejemplo, un algoritmo criptográfico específico a ser usado.

El firmante está libre de cualquier control o acción requerida en el método de firma, y puede concentrarse en leer el documento a ser firmado y en la aplicación de la clave criptográfica adecuada, con el fin de completar el proceso de firma.

Los solicitantes presentes han previsto ventajosamente que el archivo formateado pueda tener opcionalmente un formato predeterminado y que la aplicación de firma se ejecute automáticamente cuando el archivo formateado se descargue en el dispositivo electrónico.

Según un aspecto de la invención, la información incluida en el archivo formateado también comprende una acción a ser realizada después de que el documento se haya firmado, por ejemplo enviando un mensaje de correo a una dirección predeterminada asociada a un servidor de firma digital y/o el servidor que proporciona el servicio solicitado por el firmante.

El método inventivo del solicitante es, por lo tanto, no solamente ventajoso en el sentido que automatiza la correcta firma digital de documentos sino que automatiza ciertas operaciones requeridas por un servicio antes o después de la firma digital. En otras palabras, tales operaciones pueden estar estrictamente correlacionadas con el método de firma digital, por ejemplo, relacionado con el algoritmo criptográfico, o un paso anterior o posterior al método de firma, como por ejemplo enviar el resultado de la firma digital. Además, el método se puede usar para ejecutar la firma digital de un usuario, o la autenticación de un usuario.

Según esta solución, dicho problema técnico anterior se resuelve por un método para automatizar una firma digital, que comprende el paso de recibir en un dispositivo electrónico de firmante una solicitud de firma digital, caracterizado porque la solicitud de firma digital comprende la transmisión de un archivo formateado al dispositivo electrónico, que comprende parámetros para la correcta ejecución de la firma digital, dicho archivo que está asociado a una aplicación de firma en el dispositivo electrónico, adecuado para detectar los parámetros del archivo formateado y para lograr la firma digital recibiendo como entrada una clave criptográfica de firmante.

Más en particular, el método para ejecutar una firma o autenticación digital comprende el paso de transmitir una solicitud de firma digital desde un servidor remoto a un dispositivo electrónico de un firmante, y se caracteriza porque incluye en la transmisión de la solicitud de firma digital un archivo formateado que comprende los parámetros para una correcta ejecución de la firma digital, y porque ejecuta una aplicación de firma digital en el dispositivo electrónico, para detectar parámetros del archivo formateado y ejecutar la firma digital según los parámetros detectados y por medio de una clave criptográfica de firmante, dicha clave que se almacena en el dispositivo electrónico o que se introduce por el firmante en el dispositivo electrónico.

Aún según la idea inventiva, el problema técnico se resuelve por un archivo formateado para la automatización de una firma digital, que comprende uno o más parámetros para una correcta ejecución de la firma digital, dichos parámetros que comprenden al menos uno entre un algoritmo criptográfico a ser usado en la aplicación de firma, un nombre de un archivo a ser cifrado y una extensión del mismo, un archivo a ser cifrado, una o más informaciones alfanuméricas para la correcta ejecución de la firma digital, una acción a ser ejecutada después de la firma digital para la transmisión de un resultado de la firma digital, dicha acción que comprende preferiblemente el envío de un mensaje de correo electrónico a una dirección predeterminada o una acción HTTP_POST.

El problema también se resuelve con una aplicación de firma digital adecuada para la ejecución en un dispositivo

electrónico del usuario o firmante y para detectar parámetros de firma desde el archivo formateado recibido en el dispositivo electrónico desde un servidor remoto y ejecutar la firma digital recibiendo como entrada una clave criptográfica almacenada en el dispositivo electrónico o enviada al dispositivo del firmante y el documento a ser firmado. En particular, la aplicación es tal como para extraer el documento a ser firmado del archivo formateado, que comprende los parámetros de firma.

La presente invención define, propone y formaliza una metodología para encapsular toda la información requerida por la aplicación de firma dentro de una estructura de datos adecuada que de hecho constituye la “solicitud de firma” de un documento dado, es decir, una estructura de datos que permite la definición de todas las operaciones a ser ejecutadas con el fin de firmar un documento y que incluye toda la información requerida para aplicar una firma y todas las operaciones a ser realizadas después de la firma.

El problema que concierne a la aplicación de una firma correcta se resuelve por el concepto inventivo, que implementa la estructura de datos que comprende el documento a ser firmado y uno o más parámetros para aplicar una firma digital correcta. Los parámetros comprenden al menos uno entre la pluralidad de factores criptográficos tales como, por ejemplo: un algoritmo criptográfico a ser usado, el formato de archivo de la firma digital a ser generada, la autoridad de certificación a la que se hace referencia, el tipo de certificado a ser usado, las acciones específicas a ser realizadas después del la firma del documento.

Las ventajas y características adicionales del presente método, del archivo formateado y la aplicación de firma según la presente invención serán evidentes a partir de la siguiente descripción, que se proporciona con propósitos ilustrativos y no limitativos solamente, con referencia a figuras adjuntas.

Breve descripción de las figuras

La figura 1 muestra un diagrama de flujo del método para ejecutar una firma digital según la presente invención,

La figura 2 muestra un ejemplo de una parte de un archivo formateado que comprende parámetros para la ejecución de la firma digital según el método de la figura 1.

Descripción detallada

En referencia a la fig. 1, se muestran esquemáticamente los pasos de un método para ejecutar una firma digital según la presente invención, y en particular para firmar digitalmente un documento por medio de un aplicación de firma 4, que recibe como entrada el documento a ser firmado y una clave criptográfica de un firmante 5. La aplicación se almacena y se ejecuta en un dispositivo electrónico del usuario o firmante, que también almacena o recibe del firmante la clave criptográfica requerida para ejecutar la firma. Por otra parte, el documento a ser firmado se envía a la aplicación de firma por un servidor remoto, que también envía la información necesaria para una correcta ejecución del método de firma.

Una firma digital se requiere, por ejemplo, para recibir servicios proporcionados por un servidor remoto 9; el servidor es accesible, por ejemplo, a través de una dirección de Internet 2, en la que también se puede descargar el documento a ser firmado. El servidor y el documento a ser firmado se almacenan en el servidor 9, que está conectado a una red, tal como Internet, y se puede acceder desde el dispositivo electrónico 1 del firmante 5, tal como un dispositivo de mano, un ordenador personal o similar, que también está conectado a la red. En particular, el dispositivo electrónico 1 está dotado con un navegador 6 o buscador, para acceder la dirección de Internet 2.

En otras palabras, la firma digital se requiere, por ejemplo, para acceder a un servicio proporcionado por el servidor web 9, al que se puede acceder en una dirección de Internet 2. Accediendo a tal dirección por medio de su dispositivo electrónico 1, el usuario puede descargar la estructura de datos para aplicar la firma de la invención, que también se llama “solicitud de firma” en la siguiente descripción. En particular, la solicitud de firma es una estructura de datos incluida en un archivo formateado que incluye tanto el documento a ser firmado como la información para firmar el documento.

Después de haber accedido al servicio a través de la dirección de Internet 2, el dispositivo electrónico 1 del firmante recibe la solicitud de firma digital 3, que se requiere para usar el servicio. La solicitud de firma se envía por ejemplo por el servidor 9 al navegador 6 del dispositivo electrónico 1. No obstante, tal solicitud 3 se puede enviar también a través de otros medios, tales como por correo electrónico, o por medio de otro servidor 8 que está conectado a la red y está dedicado a la gestión del proceso de firma requerido para ejecutar el servicio.

Según la presente invención, la solicitud de firma digital 3 comprende la transmisión de un archivo formateado al dispositivo electrónico 1, que incluye uno o más parámetros para una correcta ejecución de la firma digital, que a continuación también se llaman información para una correcta ejecución de la firma. En particular, el archivo formateado se asocia a la aplicación de firma 4 en el dispositivo electrónico 1, y la aplicación de firma 4 es tal como para detectar los parámetros en el archivo formateado y finalizar la firma digital recibiendo como entrada desde el firmante solamente su clave criptográfica.

En otras palabras, aún según la invención, la solicitud de firma digital 3 es una estructura de datos que comprende el

documento a ser firmado y uno o más parámetros requeridos para una correcta ejecución de la firma digital. En particular, el archivo que contiene la estructura de datos y que se formatea según una codificación precisa, se asocia a la aplicación de firma 4 en el dispositivo electrónico 1, y la aplicación de firma 4 es tal como para recuperar de él el documento a ser firmado y los parámetros requeridos para aplicar la firma, recibiendo, como entrada, desde un firmante, solamente su clave criptográfica.

Ventajosamente, según el método de la presente invención, la probabilidad de errores durante el proceso de firma se reduce esencialmente a cero, debido a que el firmante recibe el archivo formateado que comprende todos los parámetros a configurar para firmar y también el archivo correcto a ser firmado para realizar el servicio, en su dispositivo, y a que la aplicación de firma extrae automáticamente el archivo a ser firmado y todos los parámetros necesarios para ejecutar correctamente la firma digital, completando la firma solamente cuando el firmante inserta su clave criptográfica. En otras palabras, la única acción requerida por el firmante es la introducción de la clave criptográfica en la aplicación de firma. Si el firmante inserta erróneamente una clave errónea, por ejemplo una clave de suscripción en lugar de una clave de autenticación, la aplicación de firma interrumpe el proceso, señalando un error. Por lo tanto, también se elimina esta fuente de error. Por otra parte, según la técnica conocida, si el firmante usa un certificado incorrecto, por ejemplo, un certificado de suscripción en lugar de un certificado de autenticación, la aplicación de firma interrumpe el proceso, algunas veces indicando un error que no siempre es fácil de comprender. La invención elimina también esta fuente de error.

Según un aspecto de la presente invención, los parámetros comprenden al menos una de las siguientes informaciones:

- un algoritmo criptográfico a ser usado por la aplicación de firma 4, tal como DES, AES, etc.;

- el nombre del archivo a ser firmado y su extensión;

- el archivo a ser firmado, una o más informaciones alfanuméricas para la correcta ejecución de la firma digital.

La información alfanumérica comprende preferiblemente unos datos de tiempo, tales como la fecha de la ejecución de firma, o una acción 7 a ser realizada después de la firma digital, para transmitir el resultado de la firma digital, tal como una transmisión al servidor 9 que proporciona el servicio.

Según un aspecto de la presente invención, los parámetros comprenden al menos una de las siguientes informaciones:

- el archivo a ser firmado,

- el modo de firma (por ejemplo una colección de información que caracteriza la firma como el organismo de certificación, tipo, etc.);

- la acción específica a ser realizada en el archivo específico (por ejemplo: una firma simple, firma y mensaje de correo, firma y transmisión por acción POST).

En la práctica, a continuación de la ejecución de firma, la aplicación de firma 4 devolverá el documento firmado con información adicional, tal como el resultado del proceso y un sello de tiempo al servidor 9.

En una realización de la invención, la acción 7 a ser realizada siguiendo la firma digital comprende el envío de un mensaje de correo electrónico a una dirección predefinida o una acción HTTP_POST. En una realización modificada, la información para aplicar la firma también comprende una acción 7 a ser realizada antes del método de firma digital.

Según otro aspecto de la presente invención, el archivo formateado que representa la solicitud de firma tiene una extensión predefinida y la aplicación de firma 4 se ejecuta automáticamente cuando se recibe el archivo formateado por el dispositivo electrónico 1. Asociando la extensión del archivo formateado a la aplicación de firma, la probabilidad de errores se reduce aún más, dado que el firmante ni siquiera tiene la elección de la aplicación a ser usada para la firma. Ventajosamente, el firmante 5 solamente introduce la clave criptográfica para completar la firma digital en la aplicación de firma 4, mientras que toda la otra información se extra automáticamente del archivo formateado, por medio de la aplicación de firma.

Obviamente, la aplicación de firma puede no estar instalada en el dispositivo electrónico cuando el firmante accede a la dirección de internet que proporciona el servicio, por ejemplo, cuando accede a él por primera vez. En tal caso, según un aspecto de la presente invención, la aplicación de firma se envía por el servidor 9, después de que el firmante haya accedido a la dirección de Internet 2. En tal caso, la aplicación de firma se envía por el servidor 9 al navegador 6 del dispositivo electrónico 1.

Según otro aspecto de la presente invención, la acción 7 para transmitir el resultado de la firma digital se envía por la aplicación de firma 4 a un servidor de gestión de firma digital 8 que es diferente del servidor 9 que proporciona el servicio. En este caso, preferiblemente, la aplicación de firma 4 envía una confirmación de firma 10 y el archivo firmado también al servidor 9 que proporciona el servicio, según los parámetros especificados en el archivo

formateado.

Según una realización, el archivo formateado se implementa mediante un archivo de almacenamiento, por ejemplo un archivo .zip o .JAR. El archivo de almacenamiento comprende en un campo DATA un archivo a ser firmado y en un campo MANIFEST, los parámetros para una correcta ejecución de la firma digital. Los parámetros se insertan en un archivo XML, por ejemplo, del tipo mostrado en la figura 2. La figura 2 muestra que una etiqueta <sign_request> se usa para caracterizar el tipo de archivo XML, es decir, un archivo de solicitud de firma digital, y una etiqueta <sign_params> se usa para apuntar a la posición donde los parámetros se han de recuperar del archivo XML. En el ejemplo mostrado en la figura 2, los parámetros incluyen un número de identificación para la solicitud de firma (etiqueta <RID>), el formato a ser usado en el método de firma (etiqueta <Type>), el tipo de clave a ser usado para la firma, por ejemplo, una clave de suscripción (etiqueta <Cert_Type>) y la acción a ser realizada, por ejemplo, después de la firma (etiqueta <sign_post_Action>). La descripción anterior de un archivo XML se incluye en un archivo formateado, proporcionado para automatización de una firma digital, según la presente invención, que comprende uno o más parámetros para una correcta ejecución de una firma digital, que se detecta automáticamente por la aplicación de firma digital, con el fin de lograr la firma digital, en donde el firmante solamente tiene que introducir su clave criptográfica en la aplicación.

En lo siguiente, se resumen brevemente los principales aspectos funcionales de la presente invención:

La definición de un esquema de firma digital que usa un modelo de “solicitud de firma” para aplicar una firma digital. El esquema proporciona un dispositivo electrónico arbitrario de un firmante que recibe una solicitud de firma digital almacenada en un archivo con un formato específico, cuya extensión se asocia a una aplicación de firma residente. El archivo que representa la “solicitud de firma” comprende el documento a ser firmado, los parámetros requeridos para una correcta ejecución de la firma digital e instrucciones opcionales que se refieren a operaciones a ser ejecutadas una vez la firma se haya aplicado al documento.

Los parámetros comprenden al menos uno entre una pluralidad de factores criptográficos tales como: el formato de firma a ser usado en la aplicación de firma, el documento a ser firmado, un conjunto de información para la correcta ejecución de la firma digital tal como por ejemplo la acción específica requerida para aplicar la firma digital. La acción que sigue a la firma, que comprende la devolución del archivo firmado a través de transmisión por correo electrónico a una dirección de correo electrónico predefinida o una acción HTTP/POST.

El archivo se construye con una extensión predefinida y/o un tipo MIME específico, de modo que la aplicación de firma se ejecute automáticamente al recibir el archivo formateado en el dispositivo electrónico, en donde el firmante solamente tiene que permitir el uso de su propia clave criptográfica por la aplicación de firma para completar la firma digital. Según un aspecto de la invención, la acción de transmitir el resultado de la firma digital se realiza enviando el mismo desde la aplicación de firma a un servidor de gestión de firmas digitales. La aplicación de firma envía además una confirmación de firma y el archivo firmado al servidor que proporciona el servicio.

El archivo formateado que representa la “solicitud de firma” es un archivo de almacenamiento comprimido que contiene el documento firmado e información requerida para ejecutar la firma.

El archivo de almacenamiento comprende un archivo a ser firmado en un campo DATA, y un archivo XML en un campo MANIFEST, que incluye dichos parámetros para la correcta ejecución de la firma digital.

Ventajosamente, según la presente invención, la probabilidad de que ocurran errores durante el método de firma se reduce esencialmente a cero, dado que solamente se requiere que el firmante introduzca su propia clave criptográfica en la aplicación de firma, mientras que toda la otra información y los parámetros requeridos para ejecutar el método se incluyen en el archivo formateado. La ventaja es aún más evidente cuando un servicio se proporciona solamente posterior a una firma digital específica, es decir, una firma que requiera parámetros específicos para la ejecución de firma, dado que tales parámetros pueden estar incluidos en el archivo formateado junto con el documento a ser firmado, y el archivo formateado que se envía al dispositivo del usuario.

REIVINDICACIONES

1. Un método para crear una firma digital que comprende el paso de transmitir una solicitud de firma digital (3) desde un servidor remoto (9) a un dispositivo electrónico del firmante (1), en donde una aplicación de firma (4) y un navegador (6) se configuran para ser ejecutados en el dispositivo electrónico (1),

en donde un archivo formateado que comprende un documento a ser firmado y los parámetros para una correcta ejecución de la firma digital se incluye en la solicitud de firma digital (3),

en donde el archivo formateado tiene una extensión predefinida asociada con la aplicación de firma, y el método que comprende:

acceder a una dirección de Internet (2) del servidor remoto (9) a través del navegador (6) por el firmante;

recibir la solicitud de firma digital desde el servidor remoto (9) por el navegador (6);

ejecutar automáticamente la aplicación de firma (4) al recibir el archivo formateado en el dispositivo electrónico (1) detectando la extensión predefinida del archivo formateado, tal como para detectar los parámetros del archivo formateado y para ejecutar la firma digital según los parámetros detectados y usando una clave criptográfica del firmante para generar la firma digital, dicha clave que se almacena en el dispositivo electrónico (1) o se introduce por el firmante en el dispositivo electrónico (1); y

realizar una acción en base a los parámetros, dicha acción que incluye enviar un mensaje de correo electrónico a una dirección predeterminada definida en los parámetros o una acción HTTP_POST.

2. Un método según la reivindicación 1, caracterizado porque dichos parámetros comprenden al menos uno entre un algoritmo criptográfico a ser usado en la aplicación de firma (4), un nombre de un archivo a ser firmado y la extensión del mismo, un documento a ser firmado, una o más informaciones alfanuméricas para la correcta ejecución de la firma digital, dicha información que comprende preferiblemente datos de tiempo o una acción (7) a ser ejecutada después de la firma digital para la transmisión de un resultado de la firma digital.

3. Un método según las reivindicaciones 1, caracterizado porque el resultado de la firma digital se envía desde la aplicación de firma (4) a un servidor de gestión de firma digital (8) que está situado en un dirección predeterminada y es diferente del servidor (9) que proporciona un servicio por medio de la dirección de Internet (2).

4. Un método según la reivindicación 3, caracterizado porque dicha aplicación de firma (4) transmite además al servidor (9) una confirmación de firma (10) y un archivo firmado.

5. Un método según cualquiera de las reivindicaciones anteriores, caracterizado porque dicho archivo formateado comprende un archivo de almacenamiento, preferiblemente un archivo .zip o un archivo .JAR.

6. Un método según la reivindicación 5, caracterizado porque dicho archivo comprende, en un campo DATA, un archivo a ser firmado, y, en un campo MANIFEST, un archivo XML que incluye dichos parámetros para la correcta ejecución de la firma digital.

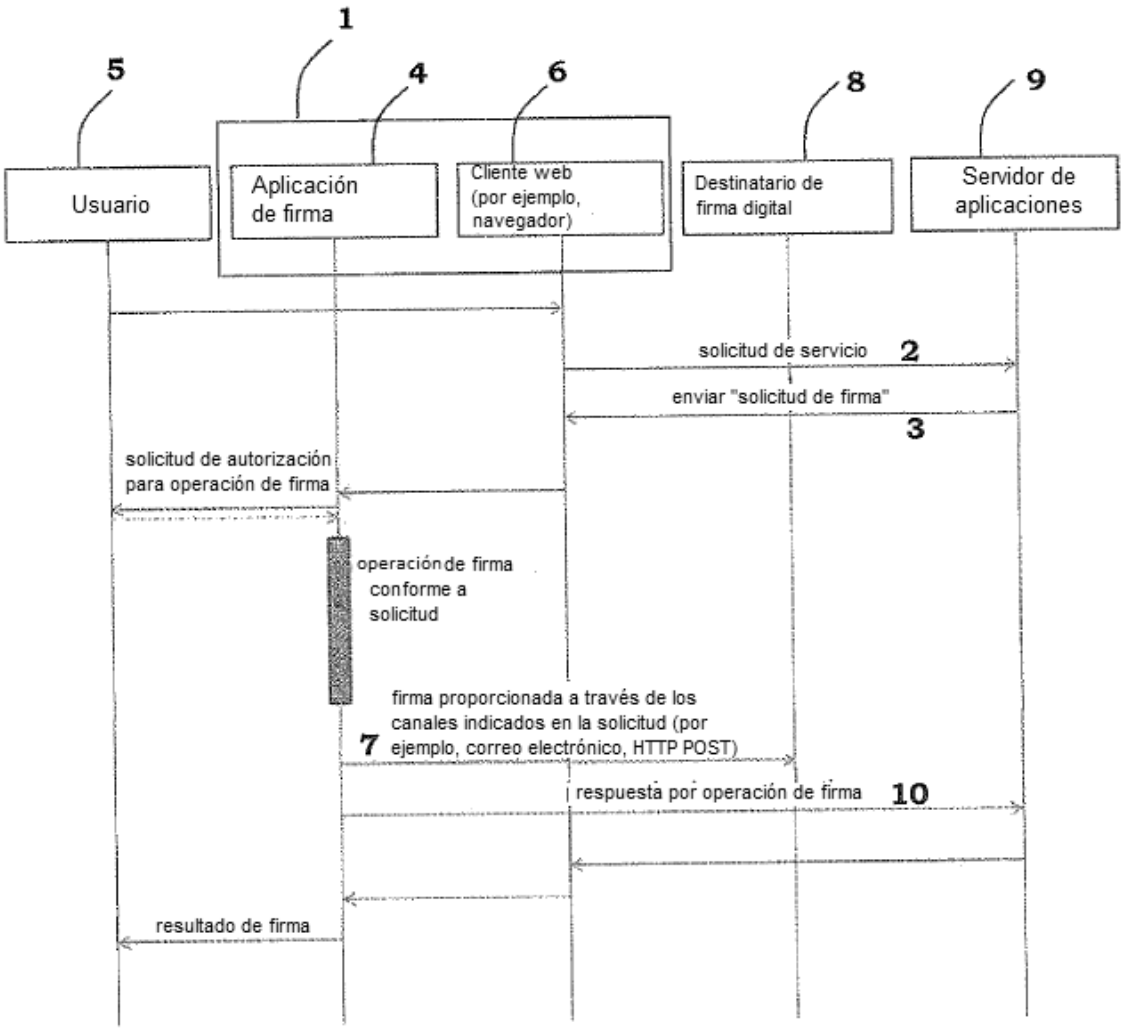
1
5
4
6
8
9
Usuario
Aplicación de firma
Cliente web (por ejemplo, navegador)
Destinatario de firma digital
Servidor de aplicaciones
solicitud de servicio 2
enviar "solicitud de firma" 3
solicitud de autorización para operación de firma
operación de firma conforme a solicitud
firma proporcionada a través de los canales indicados en la solicitud (por ejemplo, correo electrónico, HTTP POST) 7
respuesta por operación de firma 10
resultado de firma

Fig. 1

```
<?xml version="1.0" encoding="UTF-8"?>
<sign_request>
    <sign_params>
        <RID>2939837</RID>
        <Type>pades,cades</Type>
        <Cert_Type>Suscripción</Cert_Type>
        <Sign_algorithms>DSA</Sign_algorithms>
    </sign_params>
    <sign_post_Action>
        <Type>Email,HTTP_POST</Type>
        <Action>archivo firmado</ Action>
        <URL> Suscripción</URL>
    </sign_post_Action>
</sign_request>
```

Fig. 2