(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 378 080**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06764168 .8**
(96) Fecha de presentación: **13.07.2006**
(97) Número de publicación de la solicitud: **1902562**
(97) Fecha de publicación de la solicitud: **26.03.2008**

(54) Título: **Procedimiento para la entrega y archivamiento de documentos digitales**

(30) Prioridad:
13.07.2005 DE 102005033195

(45) Fecha de publicación de la mención BOPI:
04.04.2012

(45) Fecha de la publicación del folleto de la patente:
04.04.2012

(73) Titular/es:
Authentidate International AG
Rethelstrasse 47
40237 Düsseldorf, DE

(72) Inventor/es:
WENDENBURG, Jan, C. y
DAHM, Percy

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Procedimiento para la entrega y archivamiento de documentos digitales

La invención se refiere a un procedimiento para la entrega y archivamiento de documentos digitales firmados dentro de una red electrónica, así como una estructura de servidor para la comprobación de firmas en una red abierta para la realización del procedimiento.

Según la normativa europea sobre la armonización de la legislación sobe el IVA, así como regulaciones nacionales correspondientes de los estados miembros individuales de la Unión Europea empresas pueden llevar a cabo de forma totalmente electrónica los procesos de emisión de facturas. Para garantizar la legitimación de la deducción del impuesto deducible sobre el valor añadido por parte del destinatario de la factura en este caso el necesario firmar de forma electrónica las facturas electrónicas como prueba de autenticidad del origen y de la integridad del documento de factura. El nivel de calidad de las firmas electrónica a utilizar en este caso está fijado en algunos estados miembros de la Unión Europea – así, por ejemplo, en Alemania solamente los así denominados firmas electrónicas calificadas legitiman para la deducción del impuesto deducible sobre el valor añadido. Dado que se puede automatizar completamente la creación de facturas electrónicas, así como la firma de estas facturas, resultan ventajas fundamentales en el lado del emisor de la factura. Así que se puede ahorrar de forma sustancial costes de personal, pero también los costes de envío, así como los costes para la generación de la factura en papel. Estas ventajas surten efecto especialmente en el caso de grandes compañías de servicio, que facturan servicios repetitivos frente a un número elevado de clientes y en periodos regulares, tales como, compañías en el área de la telecomunicación.

Mientras que resultan ventajas importantes debido al grado elevado de automatización en la generación de facturas electrónicas para el emisor de la factura, el tratamiento de facturas electrónicas en el lado del destinatario de la factura normalmente está unido a desventajas considerables. Hay normas nacionales en las que se fija como hay que tratar facturas electrónicas firmadas en el lado del destinatario. Por ejemplo, en algunos países existe la necesidad verificar la legitimación de firma y la integridad de la factura antes de un tratamiento posterior y crear un protocolo de verificación sobre la comprobación de la firma. Además, es válido que hay que archivar todos los datos relevantes para la emisión de la factura de forma reglamentaria por parte del emisor de la factura y por parte del destinatario de la factura y que hay guardarlos en el marco del periodo de tiempo definido legalmente. Por parte del emisor de la factura esto afecta a la factura electrónica y la firma, por parte del destinatario afecta a la factura electrónica, la firma electrónica y el protocolo de verificación. El archivamiento de facturas electrónicas originales en forma de impresiones en papel expresamente no son permisibles.

Especialmente para compañías grandes el sistema para la emisión de facturas electrónicas, así como el archivamiento de facturas electrónicas y las firmas correspondientes no supone un problema esencial debido a la infraestructura informática generalmente buena. Por el contrario en el lado del destinatario frecuentemente existe el problema que no existe el ambiente técnico para la verificación de la legitimación de firma y de la integridad de la factura, así como para el archivamiento de la factura electrónica, de la firma electrónica y del protocolo de verificación. También por el lado del destinatario de la factura hay que asegurar la integridad, la exactitud, el tratamiento pronto, el orden cronológico, la ejecutoriedad, la inalterabilidad y no en último término la disponibilidad de las facturas electrónicas en el sentido de las reglas de contabilidad generalmente aceptadas. Dado que en caso de muchos destinatarios de facturas faltan las condiciones técnicas para asegurar estos criterios, esto lleva a una escasa aceptación de facturas electrónicas por parte de los destinatarios, de manera que compañías preparadas para generar electrónicamente las facturas, para firmarlas y, por ejemplo, para enviarlas a través internet mediante correo electrónico tienen que ser capaces de enviar facturas también en papel por correo ordinario.

Por el documento WO 2004/082204 A2 se conoce un procedimiento para simplificar el manejo técnico de datos firmados electrónicamente pro parte del destinatario. El núcleo que procedimiento conocido consiste en que la firma electrónica a generar para los datos a enviar antes del envío electrónico de los datos hacia el destinatario se comprueba respecto a su validez y para esta comprobación se genera un protocolo de verificación que se agrega a los datos firmados a enviar y se envía al destinatario junto con los datos a enviar. La verificación de la firma y la generación del protocolo de verificación se puede poner a disposición a través de un servicio de internet, por ejemplo, un centro de confianza que se encuentra en el flujo de datos entre el remitente y el destinatario o, por ejemplo, también mediante un servicio de servidor previsto en el lado del remitente. A través de un servicio de internet también se pueden poner a disposición del destinatario medios para retirar a través de un portal web de los datos enviados a él.

Mientras que el procedimiento conocido anteriormente es apropiado para comprobar la autenticidad de un documento digital y la autenticidad del remitente, sin embargo, no ofrece ninguna solución técnica para asegurar el archivamiento completo de documentos digitales de un remitente para el destinatario.

Por lo tanto, debido a los altos requerimientos técnicos y la infraestructura muchas veces limitada por parte del destinatario existe el problema que no es posible renunciar totalmente el papel al generar y enviar facturas. Es coste adicional causado por esto compara como desventaja con los posibles ahorros de costes y puede llevar a que una generación automática y el envío electrónico de facturas digitales no es rentable para muchas empresas.

Por el documento WO 02/21315 A1 se conoce un sistema de archivamiento de ficheros en el que el usuario en primer lugar tiene que registrarse y luego puede almacenar datos como usuario registrado. Para el archivamiento de datos en el sistema de base de datos el usuario primero tiene que inscribirse y luego puede hacer llegar un fichero al sistema de base de datos. El fichero se dispone luego de un denominado marcador electrónico (EPM) y se archiva. Este EPM puede contener un valor hash del fichero a archivar, un sellado de tiempo y/o una firma digital. El fichero poder ser retirado nuevamente del archivo por el usuario en un momento posterior, señalando sus datos de usuario y el nombre del fichero.

La tarea de la presente invención consiste en crear un procedimiento para la entrega, comprobación y archivamiento de documentos digitales firmados en redes electrónicas que se puede manejar de forma sencilla por el lado del destinatario. Esta tarea también consiste en la puesta a disposición de una estructura de servidor que posibilita un procedimiento de este tipo.

Esta tarea se resuelve con los pasos de procedimiento de la reivindicación 1.

Bajo el nombre de documento digital aquí y a continuación se entiende cualquier documento que contiene información, especialmente documentos que contienen texto, imágenes, documentos de sonido, etc.

Una red electrónica puede ser especialmente una red abierta, en donde hoy en día la internet ofrece la infraestructura adecuada para el procedimiento según la invención.

Bajo la firma digital aquí y a continuación se entiende una firma electrónica que se genera con una algoritmo de codificación asimétrico (criptografía de clave pública) que se aplica sobre documentos digitales a firmar y con la que se puede comprobar la confirmación de la integridad y la autenticidad de documento digital firmado.

Bajo archivo de datos aquí y a continuación se entiende cualquier unidad de almacenamiento en la que se pueden almacenar datos digitales. En este contexto bajo archivamiento no solo se entiende un archivamiento a largo plazo para una duración de varios años, sino también un archivamiento de datos relativamente breve.

Bajo identificador se entiende aquí y a continuación una cadena de signos que la que se puede identificar un paquete de datos de forma inequívoca.

Un núcleo esencial de la invención consiste en que para el destinatario con el identificador enviado a él es posible identificar de forma inequívoca un documento digital firmado archivado en un archivo de datos, de manera que se puede comprobar la existencia de un documento digital, su autenticidad, la autenticidad de su remitente etc. en caso de una auditoría. La posibilidad de comprobación se garantiza porque el identificador está firmado al igual que el documento digital.

Por lo tanto, el destinatario solamente tiene que almacenar el identificador alternativamente de forma electrónica o en papel para poder presentar una prueba inequívoca para la existencia y el lugar de un documento digital que le han entregado, conociendo la dirección de red del archivo de datos. Con ello el destinatario, no obstante, es capaz de beneficiarse de las ventajas de un tratamiento de datos electrónicos de forma automatizada sin la infraestructura técnica costosa. Esto es válido tanto más que incluso para empresas muy pequeñas una conexión de internet, así como una dirección de correo electrónico son equipamiento estándar.

Una manipulación del paquete de datos asociado al identificador que está archivado en el archivo de datos, por ejemplo, mediante variación o intercambio del documento digital o mediante el intercambio del paquete de datos archivado en el archivo de datos por otro con el mismo identificador, se puede descubrir especialmente cuando al destinatario se le mande también la firma junto con el identificador, ya que en el caso de una manipulación la firma electrónica para la combinación del documento digital intercambiado y del identificador ya no es válida.

El identificador fundamentalmente puede ser generado por el remitente mismo y se le puede añadir al documento digital. Sin embargo, el identificador añadido al documento digital por el remitente también se puede solicitar por una instancia que colabora con el archivo de datos. Esto último tiene la ventaja que está asegurado sin más que un identificador para el respectivo documento firmado, otorgado por la instancia, es independiente de la persona del remitente y por lo tanto es inequívoco.

Al documento digital junto con el identificador se le puede añadir también una información sobre la dirección de red del archivo de datos. Esto tiene como ventaja que en el paquete de datos, que como tarde después de su envío por el remitente siempre es una copia del fichero original o bien del paquete de datos original, está contenida una información sobre que copia se puede considerar “original” comprobable, dado que el lugar lógico de almacenamiento de la copia a considerar como “original” está definido de forma inequívoca por la dirección de red.

Para simplificar el procedimiento también para el remitente la comprobación de la firma se puede realizar por un servidor o una estructura de servidor que o bien quienes están integrados dentro de una red electrónica. Tal servidor o bien estructura de servidor puede realizar de forma automática la comprobación de la firma para paquetes de datos para una multitud de destinatarios, Además de esto, a través de un servidor de este tipo se puede ofrecer el almacenamiento tanto de paquetes de datos como también de protocolos de verificación pertenecientes. Desde un

servidor de este tipo que asume también la función del archivo de datos entonces se puede retirar el paquete de datos almacenado en él mediante el envío del identificador asociado a él.

El servidor o bien la estructura de servidor en una realización preferida del procedimiento según la invención se puede ejercer por una instancia independiente. Bajo una instancia independiente se entiende especialmente un proveedor de servicios de internet especialmente fiable, tal como, por ejemplo, un centro de confianza cuya independencia y fiabilidad se ha certificado por el organismo apropiado.

El paquete de datos que especialmente puede ser una factura electrónica, generalmente se le envía automáticamente a destinatario por completo o en partes, sin que se retira el documento digital del archivo de datos indicando el identificador. Sin embargo, esto no es necesario obligatoriamente mientras que se asegura de otro modo que el destinatario tenga conocimiento del contenido del documento digital.

El procedimiento es especialmente apropiado para crear más manejable la discontinuidad de medio que existe entre un tratamiento de datos automático, exclusivamente de forma electrónica y un tratamiento de datos basado en papel. De este modo el documento digital inclusive de las indicaciones añadidas con respecto al archivo de datos y con respecto al identificador se puede imprimir sobre papel por o bien para el destinatario, en donde la impresión representa una referencia para el documento digital tratado de forma reglamentaria.

La tarea mencionada anteriormente también se resuelve con una estructura de servidor para la comprobación de firma dentro de una red abierta con las características de la reivindicación 12.

Bajo medios aquí y a continuación se entiende especialmente componentes electrónicos de un ordenador, ordenadores o varios ordenadores interactuando que realizan una determinada función. Como se tiene que procurar o como de tiene que describir mediante software estos medios para la realización de una determinada función el experto conoce ampliamente, de manera que en este lugar no se explica más en detalle.

La estructura de servidor requerida que puede consistir de uno o varios ordenadores o bien servidores integrados en la red abierta puede hacerse cargo de todas las tareas a realizar relacionadas con la comprobación de la firma, especialmente la comprobación de firma y la generación del protocolo de verificación con respecto a la comprobación de la firma, el añadir del protocolo de verificación y en su caso del identificador al paquete de datos, el almacenamiento o bien archivamiento de los documentos firmados de forma electrónica, el aviso del destinatario sobre la presencia de un documento firmado de forma electrónica mediante el envío al destinatario de al menos el identificador añadido al documento digital y en su caso del documento digital electrónicamente firmado, en donde el envío del documento digital electrónicamente firmado al destinatario se puede realizar de forma automática o a solicitud del destinatario opcionalmente con y sin protocolo de verificación.

Una estructura de servidor como esta también puede estar dotada de medios para la generación y para el envío al destinatario de un identificador inequívoco. Estos medios, por ejemplo, pueden fijar números correlativos como identificador o, sin embargo, pueden generar cualquier secuencia de cifras o números como identificador con la ayuda de un generador de números aleatorios, en donde hay que comprobar entonces si la secuencia cualquiera de cifras o números ya se había fijado anteriormente.

A continuación se describe la invención más en detalle con la ayuda de una figura que muestra un ejemplo de realización preferente de la invención.

Figura 1 muestra un diagrama para la explicación del transcurso de un procedimiento preferido, a modo de ejemplo según la invención.

En una estructura de servidor 1 de un remitente se genera un documento digital D. Además de esto, se solicita un identificador ID por una estructura de servidor para la comprobación de la firma 2 que presenta un generador de ID 3, que contiene una cadena de signos inequívoca, especialmente aleatoria y se lo añade al documento digital D. A ambos se les provee de una firma electrónica S. Un paquete de datos que consiste del documentos digital, el identificador ID y la firma electrónica S se envía a través de internet hacia una estructura de servidor para la comprobación de la firma 2.

La estructura de servidor para la comprobación de la firma 2 comprende medios para el tratamiento reglamentario del paquete de datos 5, especialmente para la comprobación de la firma S del documento digital D y para la generación de un protocolo de verificación P sobre la comprobación de la firma. Además, la estructura de servidor 3 comprende un generador de ID 5 que genera un identificador I para cada paquete de datos a tratar o bien tratado. Finalmente la estructura de servidor comprende también un archivo de datos 6 para la comprobación de la firma 3. En este archivo de datos 6 se almacenan los paquetes de datos ampliados, en cada caso, por un identificador I y un protocolo de verificación P.

El documento digital D, así como el identificador I que está asociado al paquete de datos que contiene el documento digital D se envía a un ordenador destinatario 7 por la estructura de servidor 3. El destinatario ahora tiene la posibilidad de pedir todos los datos asociados al documento digital D que están almacenados en el archivo de datos

6, transmitiendo el identificador I hacia la estructura de servidor 3 para la comprobación de la firma.

La estructura de servidor entonces envía a petición los datos almacenados en el archivo de datos 6, especialmente el documento digital D, la firma S del documento digital D, el protocolo de verificación P y el identificador I hacia un ordenador del destinatario 8 que puede ser el mismo ordenador que el ordenador destinatario 7 o también puede ser un ordenador de un auditor 8.

Como prueba de la presencia del documento digital firmado y del protocolo de verificación sobre la comprobación de la firma el destinatario, por ejemplo, puede generar una impresión PD en papel del documento digital en el que se imprime la secuencia de signos del identificador I, en su caso junto con la información de red respecto a la dirección de red del archivo de datos.

Este procedimiento se puede variar de forma múltiple, de lo que pueden resultar también ventajas adicionales. De este modo la firma del paquete de datos y la colocación de la firma al paquete de datos no tiene por qué realizarse de forma obligatoria en el remitente, sino se puede realizar por un servicio “externo” como la estructura de servidor 2. De forma inversa una vez generada la firma en el remitente también se puede realizar en el remitente la comprobación de la firma junto con la generación del protocolo de verificación para la comprobación de la firma y el agregado del protocolo de verificación al paquete de datos. De la misma manera se puede generar la ID en el lado del remitente y se le puede añadir al paquete de datos. Sobre todo es crucial que le identificador y el documento digital se firman junto electrónicamente y la firma se le añade al paquete de datos.

REIVINDICACIONES

1. Procedimiento para la entrega y el archivamiento de documentos digitales firmados dentro de una red electrónica en el que

   - se genera un paquete de datos digital que contiene al menos un documento digital de un remitente;
   - se firma de forma digital el paquete de datos y la firma digital se le añade al paquete de datos;
   - se comprueba la validez de la firma digital en el marco de una comprobación de la firma y se genera un protocolo de verificación sobre la comprobación de la firma;
   - el protocolo de verificación se añade al paquete de datos; y
   - se transmite el paquete de datos hacia un archivo de datos;

   caracterizado porque

   - antes de la firma digital del paquete de datos digital se genera un identificador que identifica de forma inequívoca al documento digital y se le añade al paquete de datos digital, y
   - a un destinatario del documento digital firmado se le transmite al menos el identificador y un aviso sobre el archivo de datos, en donde el destinatario puede obtener el paquete de datos desde el archivo de datos indicando al menos el identificador.

2. Procedimiento según la reivindicación 1, caracterizado porque se le transmite al destinatario la firma electrónica.

3. Procedimiento según la reivindicación 1 o 2, caracterizado porque al documento digital junto con el identificador se le añade un aviso sobre la dirección de red del archivo de datos.

4. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque el identificador contiene una secuencia de signos aleatoria pero inequívoca cuya simple indicación le permite al destinatario el acceso al paquete de datos en el archivo de datos.

5. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque la comprobación de la firma se realiza por una instancia independiente.

6. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque el archivamiento se realiza por una instancia independiente y el archivo de datos se gestiona especialmente por una instancia independiente.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque el identificador es generado por una instancia independiente.

8. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque la comprobación de la firma solamente se realiza y el protocolo de verificación sobre la comprobación de la firma solamente se genera cuando el destinatario obtiene el paquete de datos del archivo de datos.

9. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque el documento digital es una factura digital.

10. Procedimiento según la reivindicación 3 o una reivindicación que se refiere a esta, caracterizado porque el documento inclusive los avisos añadidos respecto al archivo de datos y al identificador se imprime sobre papel y porque la impresión representa una referencia hacia el documento digital empleado reglamentariamente.

11. Procedimiento según una cualquiera de las reivindicaciones anteriores, caracterizado porque la red electrónica es una red abierta, especialmente el internet.

12. Estructura de servidor para la comprobación de firma dentro de una red abierta para la realización de un procedimiento según una cualquiera de las reivindicaciones anteriores con

    - medios para recibir un paquete de datos desde un remitente, en donde el paquete de datos contiene al menos información respecto a la identidad del remitente, datos con respecto a la dirección de la red del destinatario, así como al menos un documento digitalmente firmado dotado de un identificador,
    - medios para la comprobación de la validez de la firma en el marco de una comprobación de la

firma,

- medios para la generación de un protocolo sobre la comprobación de la firma,
- medios para añadir el protocolo de verificación al paquete de datos,
- medios para la gestión adicional incluyendo el almacenamiento del paquete de datos, y
- medios para enviar al menos el identificador e indicaciones respecto a la dirección de red de los medios de almacenamiento hacia la dirección de red del destinatario.

13. Estructura de servidor según la reivindicación 12, caracterizado por medios para la generación de un identificador para el paquete de datos a petición del remitente y para el envío del identificador hacia el destinatario.

14. Estructura de servidor según la reivindicación 12 o 13, caracterizado por medios para la generación de una firma electrónica para un paquete de datos.

15. Estructura de servidor según una cualquiera de las reivindicaciones 12 a 14, caracterizado por

- medios para la recepción de un identificador por el destinatario para la retira de un paquete de datos inclusive del protocolo de verificación;
- medios para asignar el identificador al paquete de datos almacenado;
- medios para enviar el paquete de datos junto con el protocolo de verificación hacia la dirección de red del destinatario.

16. Estructura de servidor según una cualquiera de las reivindicaciones 12 a 15, caracterizado porque los medios de almacenamiento comprenden medios para el archivamiento de paquete de datos.

17. Estructura de servidor según una cualquiera de las reivindicaciones 12 a 16, caracterizado por el menos un ordenador.

18. Estructura de servidor según una cualquiera de las reivindicaciones 12 a 17, caracterizado por una conexión a internet.

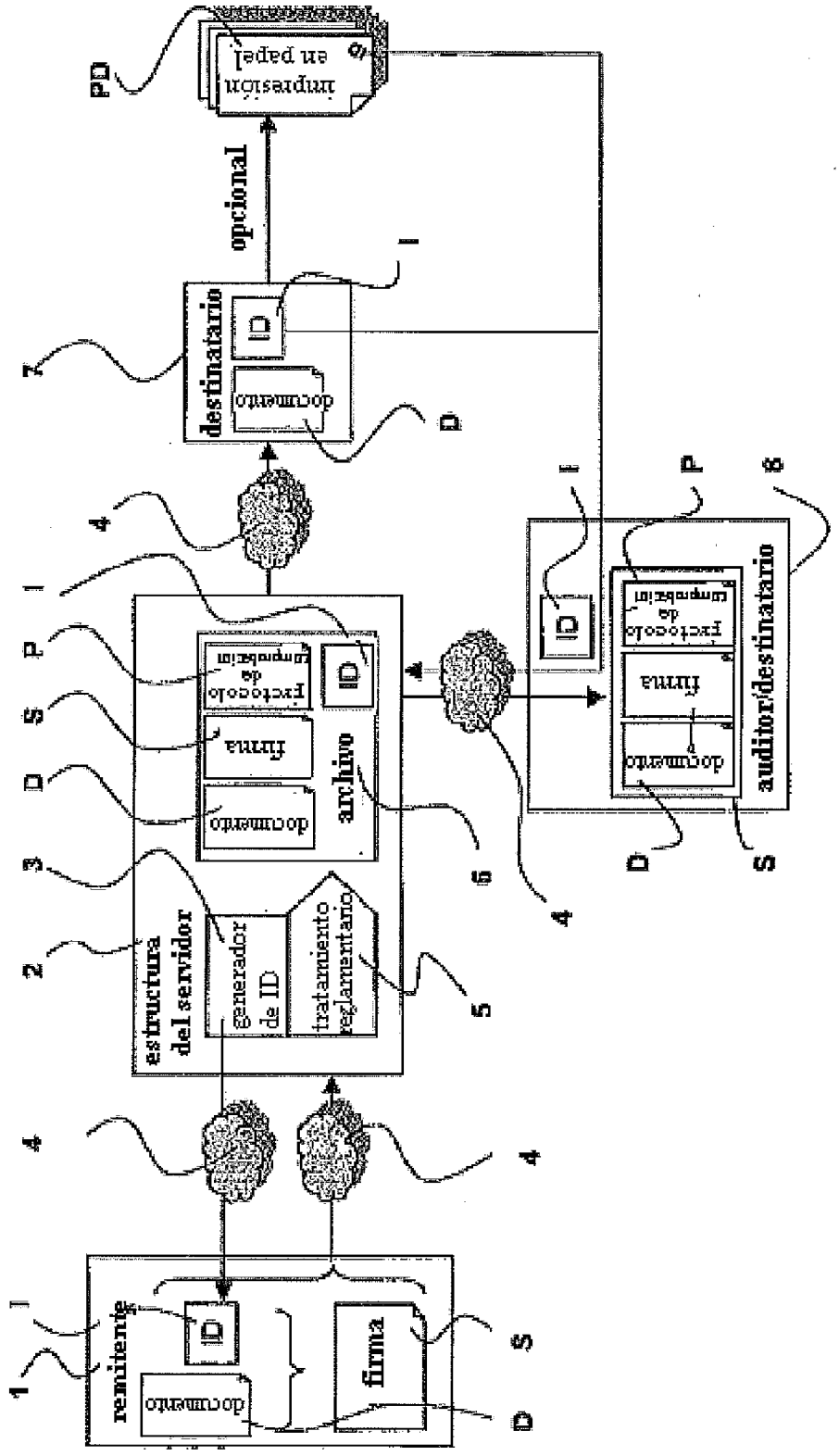
remitente
ID
documento
firma
estructura del servidor
generador de ID
tratamiento reglamentario
archivo
ID
documento
firma
fructoscolo de comprobación
destinatario
ID
documento
auditor/destinatario
ID
documento
firma
fructoscolo de comprobación
opcional
impresión en papel
PD
1
2
3
4
5
6
7
8
D
S
P
I

Figura 1