

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 991 390**

51 Int. Cl.:

H04L 9/32 (2006.01)

H04W 12/08 (2011.01)

H04L 9/40 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **15.10.2021** **E 21306442 (1)**

97 Fecha y número de publicación de la concesión europea: **21.08.2024** **EP 4167520**

54 Título: **Certificación digital de documentos escaneados**

45 Fecha de publicación y mención en BOPI de la
traducción de la patente:
03.12.2024

73 Titular/es:

AMADEUS S.A.S. (100.0%)
485 route du Pin Montard, Sophia Antipolis
06410 Biot, FR

72 Inventor/es:

VON SCHLEDORN, MARTIN;
BILDNER, SEBASTIAN;
SASIDHARAN, RENJITH K;
PARIDA, SWAGAT y
STARK, THOMAS

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 991 390 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Certificación digital de documentos escaneados

Campo

5 La presente invención se refiere a un sistema y método para certificar y almacenar digitalmente copias digitales de documentos escaneados.

Antecedentes

10 Las copias digitales de documentos originales se usan en una gama de aplicaciones que implican el procesamiento digital y la transmisión de la información contenida en un documento original, por ejemplo, archivado digital, informe de gastos digitales, y similares. En muchos casos, se requiere mantener el documento original para probar la autenticidad de la copia digital correspondiente. Por ejemplo, cuando se presenta un informe de gastos digitales para reembolso que contiene imágenes digitales de recibos escaneados recogidos durante un periodo de tiempo, es necesario mantener los recibos originales con el fin de demostrar la autenticidad de la información contenida en el informe de gastos, por ejemplo, en el caso de una auditoría fiscal.

15 La razón para mantener los documentos originales es porque las copias digitales de documentos escaneados pueden modificarse fácilmente usando una aplicación de software apropiada. Por ejemplo, un usuario que presenta un informe de gastos puede escanear documentos originales usando la cámara de un dispositivo electrónico para obtener imágenes digitales correspondientes, que pueden procesarse usando el software deseado antes de que se transmitan a un servicio de informe de gastos para reembolso. Sin embargo, antes de presentar las imágenes digitales, se presenta al usuario la oportunidad de modificar la información representada en las mismas. Por ejemplo, el usuario puede procesar posteriormente las imágenes digitales para alterar las cantidades citadas en las copias digitales de los recibos, cambiar información tal como la fecha o la hora, y similares. Como resultado, las copias digitales de documentos originales se consideran vulnerables al comportamiento ilícito y requieren mantener las copias originales correspondientes.

25 Un sistema y método de ejemplo del estado de la técnica para crear copias certificadas de documentos originales se describe en el documento US 2006/0259783 A1. El método comprende autenticar a un usuario, proporcionar una primera versión digital de la información original, certificar que una segunda versión digital es la misma que la primera versión, y comparar las huellas digitales de ambas versiones digitales para asegurar que son las mismas, proporcionando de este modo una copia certificada.

30 Un ejemplo de un sistema y método para la recogida, captura, procesamiento, almacenamiento y seguimiento de datos se describe en el documento US 2018/0075410 A1. Las copias de imagen digitales modificables se comparan con la fuente en papel, y cuando se determina que es una copia exacta certificada por el adjunto de una firma electrónica. Un sistema y un método de ejemplo para validar electrónicamente documentos escaneados se describe en el documento US 2006/0224895 A1. Un documento electrónico se firma con una firma electrónica del usuario y del aparato de formación de imágenes y se valida mediante la firma del documento usando una firma electrónica del notario eléctrico.

35 Por lo tanto, existe la necesidad de proporcionar una solución mejorada para garantizar la autenticidad de copias digitales de la solución de documentos escaneados.

Compendio de la invención

40 Un objetivo de la presente invención es garantizar la autenticidad de la información presentada en copias digitales de documentos originales y garantizar además que las copias digitales certificadas se almacenen en una base de datos fiable y accesible que mantiene el orden cronológico en donde se crearon y/o enviaron las copias digitales certificadas para su procesamiento.

45 El objetivo de la presente invención se consigue según el sistema, método y producto de programa informático que muestran las características de las reivindicaciones independientes. Las realizaciones preferidas se describen en las reivindicaciones dependientes.

Según un aspecto de la presente invención, se presenta un método para certificar la autenticidad de copias digitales de documentos originales en un servidor de certificación de datos, comprendiendo el método:

50 recibir, de una aplicación de cliente que se ejecuta en un dispositivo electrónico de un usuario, una carga útil de datos firmados digitalmente y un documento electrónico firmado digitalmente correspondiente asociado con un documento original,

en donde el documento electrónico firmado digitalmente comprende una copia digital de un documento original que contiene una o más páginas y una firma digital generada,

y en donde la carga útil de datos firmados digitalmente comprende el documento electrónico firmado digitalmente, elementos de datos asociados con el documento original y una firma digital generada; y

certificar y almacenar la carga útil de datos firmados digitalmente recibidos y el documento electrónico correspondiente realizando las etapas de:

- 5 recalcular las firmas digitales correspondientes para la carga útil de datos firmados digitalmente y el documento electrónico y comparar las firmas recalculadas con las firmas digitales aplicadas en la aplicación de cliente;

en respuesta a la determinación de que el documento electrónico y la carga útil de datos coinciden, autenticar el documento electrónico y la carga útil de datos correspondiente aplicando un certificado de autenticación, que se recupera de una base de datos de certificación del servidor de certificación;

- 10 generar, en una parte de una base de datos fiable asociada con el usuario y/u organización de usuario vinculada a la aplicación de cliente, un registro de datos (247_1-n) que comprende el documento electrónico autenticado y elementos de datos asociados obtenidos a partir de la carga útil de datos autenticados; y

devolver un número de identificación único y una marca de tiempo asociada a la generación del registro de datos.

- 15 La solución presentada en el presente documento permite la certificación de copias digitales de documentos originales comparando las firmas digitales del documento electrónico y la carga útil de datos generada en la aplicación de cliente, con las correspondientes firmas digitales recalculadas generadas en el servidor de certificación. La firma digital de al menos la carga útil de datos se calcula en base a los datos contenidos en la misma, incluyendo la firma digital del documento electrónico. Como resultado, cualquier cambio realizado en la carga útil de datos y/o el documento electrónico después de que se haya aplicado la firma digital se reflejaría en las firmas recalculadas correspondientes
- 20 en el servidor de certificación. Por lo tanto, cualquier cambio posterior a la modificación en el documento electrónico y/o carga útil de datos conduciría a un error en el procedimiento de autenticación en el servidor de certificación, que puede activar una alerta a un usuario registrado, por ejemplo, en la aplicación de cliente. De esta manera, es posible detectar cambios posteriores a la modificación realizados en el documento electrónico y garantizar la autenticidad de la información transmitida, que al menos incluye la carga útil de datos y el documento electrónico. Los elementos de
- 25 datos contenidos en la carga útil de datos pueden extraerse directamente de las copias digitales de los documentos originales y/o proporcionarse por el usuario. Los elementos de datos pueden incluir un rango de información asociada con el documento original y/o el usuario. Por ejemplo, los elementos de datos asociados con recibos escaneados pueden incluir información extraída de imágenes de los recibos originales, tales como la fecha, hora, elementos adquiridos y cantidades correspondientes. Al mismo tiempo, el usuario puede añadir además información adicional tal
- 30 como información personal, código fiscal, detalles de pago y similares. Según la presente divulgación, el usuario de la aplicación de cliente puede estar provisto de un menú para añadir la información necesaria y/o verificar la información extraída de las copias digitales de los documentos originales escaneados. Las copias digitales pueden estar en forma de imágenes obtenidas usando una cámara de un dispositivo electrónico que ejecuta la aplicación de cliente. Cada imagen puede representar una copia digital de una página de un único documento original. Las copias digitales
- 35 obtenidas del documento original correspondiente se combinan en un único archivo electrónico que tiene un primer formato de datos, por ejemplo, formato de documento portátil (PDF). Cada página en el documento electrónico puede representar una copia digital de una página de un documento original, y se pueden añadir más páginas según sea necesario. Como tal, se generaría un documento electrónico independiente para cada documento original, por ejemplo, un recibo de gastos basado en papel tal como una factura de restaurante, y similares. Cada documento electrónico
- 40 estaría certificado y almacenado en la base de datos fiable como una entrada independiente.

- 45 Según realizaciones de la presente divulgación, la etapa de generación de un registro de datos comprende la etapa de generación de un nuevo bloque de datos en un libro de registro digital de la base de datos fiable asociada con el usuario y/o organización de usuario a la que está vinculada la aplicación de cliente, estando dispuesto cada bloque de datos del libro de registro digital en orden cronológico según la información de marca de tiempo del registro de datos correspondiente.

- 50 El documento electrónico autenticado, junto con al menos una parte de los elementos de datos contenidos en la carga útil de datos autenticados, se almacenan como un registro de datos en una parte de la base de datos fiable asociada con el usuario y/o organización de usuario vinculada con la aplicación. Cada registro de datos puede estar en forma de un nuevo bloque de datos en un libro de registro de base de datos de la parte de la base de datos fiable. El libro de datos puede basarse en una tecnología de libro de datos existente, tal como una cadena de bloques o similar, donde cada bloque de datos está provisto de una firma digital única y una marca de tiempo que indica cuándo se creó el bloque de datos en el libro de datos. La marca de tiempo puede ser una secuencia de caracteres o información codificada que identifica cuándo se produjo un evento dentro del libro de registro de la base de datos y proporciona información tal como hora, fecha y similares. Cada bloque de datos del libro de registro digital está dispuesto en orden
- 55 cronológico según la información de marca de tiempo del registro de datos correspondiente. El libro de registro digital mantiene el seguimiento de los bloques de datos creados y su orden cronológico, evitando de este modo que se realicen y/o registren cambios en la información contenida en los bloques de datos.

Según realizaciones de la presente divulgación, la carga útil de datos se envuelve en un testigo de autenticación que se firma digitalmente usando una firma digital calculada a partir de datos contenidos en la carga útil de datos y una clave criptográfica compartida entre la aplicación de cliente y el servidor de certificación. El testigo de autenticación puede ser un testigo web JSON o similar que contiene una firma digital y/o cifrado de los datos contenidos en la carga útil de datos. Como resultado, cualquier intento de cambiar los datos contenidos en el testigo de autenticación se reflejaría en el recálculo de la firma digital correspondiente realizado en el servidor de certificación. De esta manera, la solución descrita en el presente documento proporciona salvaguardas adicionales para evitar modificaciones posteriores fraudulentas de los datos en la carga útil de datos y/o el documento electrónico.

Según realizaciones de la presente divulgación, la firma digital de la carga útil de datos y/o el documento electrónico puede calcularse usando una función hash tal como el algoritmo de función hash SHA-256 o similar junto con una clave compartida.

Según realizaciones de la presente divulgación, a cada bloque de datos en el libro de registro digital se le asigna una firma digital única calculada basándose en al menos las firmas digitales del documento electrónico y la carga útil de datos almacenada en el registro de datos. Además, la firma digital de cada bloque de datos en el libro de registro digital puede basarse además en la firma digital de un bloque de datos anterior en el libro de registro digital. Por ejemplo, la firma digital de un bloque de datos puede calcularse en base a la firma digital y/o el valor criptográfico de uno o más elementos de datos en la tabla dedicada, por ejemplo, el primer elemento de datos y/o las firmas digitales asignadas a la carga útil de datos y el documento electrónico. Como tal, cualquier modificación posterior, hecha a los datos extraídos del documento original se reflejaría en la firma digital del bloque de datos, proporcionando así salvaguardas adicionales para prevenir y detectar modificaciones posteriores hechas a la información almacenada en la base de datos fiable. En general, la presente divulgación proporciona un mecanismo para garantizar que los bloques de datos que contienen los datos certificados no pueden eliminarse, alterarse o reordenarse sin romper la integridad del libro de registro de base de datos, lo que activaría una alerta que indica actividad fraudulenta.

Según realizaciones de la presente divulgación, el servidor de certificación está configurado para autenticar la información contenida en los bloques de datos creados en el libro de registro digital asociado con el usuario durante un marco de tiempo especificado realizando las etapas de:

recuperar, en base al orden cronológico de bloques de datos, la firma digital única del primer y último bloque de datos en el libro de registro digital asociado con el marco de tiempo especificado;

calcular, basándose en firmas digitales recuperadas, una firma de cierre para el marco de tiempo especificado; y

aplicar un certificado de autenticación a la firma de cierre calculada, que se recupera de la base de datos de certificación.

El servidor de certificación está configurado para autenticar la información contenida en bloques de datos creados en el libro de registro digital asociado con el usuario durante un marco de tiempo especificado, por ejemplo, un período de contabilidad o similar. La solución de la presente divulgación ofrece la posibilidad de agregar información de diferentes bloques de datos asociados con un marco de tiempo especificado. Por ejemplo, en el caso de informes de gastos, es habitual recoger y agregar información de los informes de gastos enviados para reembolso a lo largo de un período de contabilidad. La presente solución permite cerrar los periodos actuales y crear nuevos periodos de contabilidad en el libro de registro de la base de datos para cada cliente en base a la configuración del cliente, por ejemplo, en base a la información de contabilidad que se aplica para cada cliente. Cada período de contabilidad se cierra mediante una firma digital de cierre generada basándose en las firmas digitales obtenidas del primer y último bloque de datos en el libro de registro distribuido asociado con el marco de tiempo especificado, por ejemplo período de contabilidad. Al final de cada período de tiempo especificado, se crea un bloque de datos de final de período en el libro de registro digital que contiene la firma de cierre generada y una certificación de autenticación para indicar la autenticidad de los datos contenidos en los bloques de datos del marco de tiempo especificado. El bloque de datos de final de período indica el punto de cierre de un marco de tiempo especificado y el punto de inicio de otro, por ejemplo, un período de contabilidad de impuestos. La información contenida en la firma digital de cierre del bloque de datos de final de período puede usarse para verificar las transacciones individuales grabadas en cada bloque de datos anterior asociado con el marco de tiempo especificado, sin la necesidad de comprobar individualmente cada bloque en la cadena.

Según realizaciones de la presente divulgación, la etapa de aplicar el certificado de autenticación al documento electrónico autenticado comprende las etapas de:

convertir el documento electrónico autenticado de un primer formato digital a un segundo formato digital predefinido;

añadir metadatos al documento electrónico convertido.

El servidor de certificación, antes de aplicar un certificado de autenticación a la carga útil autenticada y al documento electrónico, convierte el documento electrónico del primer formato digital a un segundo formato digital, por ejemplo, de PDF a PDF/A o equivalente. Además, durante la conversación del documento electrónico, se añade un conjunto de información de metadatos al documento electrónico, tal como versión de aplicación de cliente, fecha/hora de

captura, nombre de software, versión de software y similares.

Según realizaciones de la presente divulgación, la etapa de recuperar un certificado de autenticación de la base de datos de certificación comprende las etapas de:

- 5 comprobar la validez del certificado de autenticación seleccionado emitiendo, a través de un enlace incluido en cada certificado de autenticación, una solicitud a un servicio de certificación para comprobar la validez y/o el estado de revocación del certificado de autenticación seleccionado;

en donde si la respuesta recibida del servicio de certificación indica que el certificado seleccionado es inválido y/o revocado, el servidor de certificación está configurado para realizar las etapas de:

eliminar el certificado no válido de la base de datos de certificados;

- 10 seleccionar un nuevo certificado de autenticación de la base de datos de certificados; y
comprobar la validez del nuevo certificado de autenticación.

Según realizaciones de la presente divulgación, el servidor de certificación puede configurarse para solicitar la emisión de nuevos certificados de autenticación desde el servicio de certificación para almacenarse en la base de datos de certificados

- 15 Según realizaciones de la presente divulgación, la etapa de determinar la autenticidad del documento electrónico y la carga útil de datos comprende las etapas de:

recalcular la firma digital aplicada a la carga útil de datos en función de los datos contenidos en la carga útil de datos y de una clave criptográfica compartida, y comparar la firma digital recalculada con la firma digital de la carga útil de datos;

- 20 en respuesta a la determinación de que la firma recalculada es igual a la firma digital de la carga útil de datos, extraer de la carga útil de datos validada el valor hash del documento electrónico; y

comparar el valor hash extraído de la carga útil de datos validada con el valor hash recalculado del documento electrónico firmado recibido en el servidor de certificación.

- 25 Según realizaciones de la presente divulgación, la etapa de devolver un número de identificación único y una marca de tiempo asociada con la generación del registro de datos comprende la etapa de comunicar una copia del registro de datos a una o más aplicaciones de cliente conectadas

El certificado de autenticación aplicado a la carga útil de datos autenticados, y el documento electrónico también se pueden aplicar a la firma de cierre digital del bloque de datos de cierre generado para cada marco de tiempo especificado en el libro de registro distribuido. El certificado de autenticación se selecciona de una base de datos de certificación que comprende una pluralidad de certificados de autenticación obtenidos de un servicio de certificación, que puede ser parte del servidor de certificación y/o servicio de terceros. Antes de aplicar el certificado de autenticación, el servidor de certificación comprueba la validez del certificado contactando con el servicio de certificación a través de un enlace integrado proporcionado en cada certificado de autenticación. En el caso de una respuesta negativa del servicio de certificación que indica que el certificado de autenticación seleccionado no es válido o se revoca, el servidor de certificación selecciona un nuevo certificado de la base de datos.

- 30 Según un segundo aspecto de la presente divulgación, se proporciona un sistema para certificar la autenticidad de copias digitales de documentos originales, comprendiendo el sistema:

una aplicación de cliente que se ejecuta en un dispositivo electrónico de un usuario configurada, en respuesta a la recepción de una solicitud de certificación de un usuario para certificar una copia digital de un documento original, para

- 40 adquirir una copia digital de cada página del documento original a certificar y los datos correspondientes,

generar un documento electrónico de un primer formato digital que contiene las copias digitales adquiridas asociadas a las páginas del documento original y una carga útil de datos que comprende el documento electrónico generado y los elementos de datos asociados al documento original,

- 45 firmar digitalmente la carga útil de datos y el documento electrónico calculando una firma digital correspondiente para la carga útil de datos y el documento electrónico, en donde la firma digital del documento electrónico se añade a los datos contenidos en la carga útil de datos, y

comunicar la carga útil de datos firmados y el documento electrónico firmado al servidor de certificación de datos; y

- 50

un servidor de certificación acoplado comunicativamente a la aplicación de cliente configurado, en respuesta a la recepción de la carga útil de datos firmados y el documento electrónico firmado, para realizar las etapas del método según las realizaciones del primer aspecto.

5 Según realizaciones de la segunda realización, la aplicación de cliente está configurada para firmar digitalmente la carga útil de datos al envolver la carga útil de datos en un testigo de autenticación, comprendiendo el testigo de autenticación una firma calculada en base a los datos contenidos en la carga útil de datos y una clave criptográfica compartida entre la aplicación de cliente y el servidor de certificación.

Según realizaciones de la segunda realización, la aplicación de cliente está configurada para firmar digitalmente la carga útil de datos calculando adicionalmente un hash para el documento electrónico usando una función hash.

10 Según realizaciones de la segunda realización, los documentos originales y las copias digitales correspondientes están en forma de recibos de gastos basados en papel que comprenden información de gastos. Debe observarse que otros tipos de documentos pueden certificarse usando el método y el sistema de la presente divulgación.

15 Según realizaciones de la segunda realización, la base de datos fiable del servidor de certificación se divide en una pluralidad de partes, cada una asociada con un usuario y/u organización de usuario vinculada con la aplicación de cliente. Al dividir la base de datos fiable en partes independientes, se tiene la ventaja de un mantenimiento más fácil, ya que solo se necesita mantener una base de datos, mientras se garantiza la segregación de información entre diferentes usuarios.

20 Según realizaciones de la segunda realización, el servidor de certificación está configurado para identificar, en base a la información transmitida desde la aplicación de cliente, la identidad del usuario y/u organización del usuario y, en consecuencia, dirigir datos a la parte correspondiente de la base de datos fiable.

25 Según un aspecto adicional de la presente divulgación, se proporciona un producto de programa informático que comprende instrucciones de código de programa almacenadas en un medio legible por ordenador, que cuando se ejecutan por un módulo procesador del servidor de certificación en respuesta a la recepción de una solicitud de una aplicación de cliente para certificar una carga útil de datos firmados y un documento electrónico firmado, hacen que el servidor de certificación realice la etapa de certificación y almacenamiento de la carga útil de datos recibida y el documento electrónico según realizaciones del primer aspecto.

Breve descripción de los dibujos

Los siguientes dibujos se proporcionan como un ejemplo para explicar adicionalmente y describir diversos aspectos de la invención:

30 La figura 1 muestra una implementación ejemplificada de un sistema para certificar la autenticidad de copias digitales de documentos originales según realizaciones de la presente divulgación.

La figura 2 muestra una arquitectura de sistema ejemplificada del servidor de certificación del sistema de la figura 1 según realizaciones de la presente divulgación.

35 La figura 3 muestra una implementación ejemplificada de un sistema de certificación de gastos según realizaciones de la presente divulgación.

La figura 4 muestra una implantación ejemplificada de un libro de datos de base de datos fiable según las realizaciones de la presente divulgación.

La figura 5 muestra un método ejemplificado para certificar la autenticidad de copias digitales de documentos originales según realizaciones de la presente divulgación.

40 Descripción detallada

La presente invención se ilustrará usando las realizaciones ejemplificadas mostradas en las figuras, que se describirán con más detalle a continuación. Debe observarse que cualquier referencia hecha a las dimensiones es solo indicativa y no restringe la invención de ninguna manera. Aunque esta invención se ha mostrado y descrito con referencia a ciertas realizaciones ilustradas de la misma, los expertos en la técnica entenderán que pueden realizarse diversos cambios en la forma y detalles en la misma sin alejarse del alcance de la invención.

45 La figura 1 muestra una implementación ejemplificada de un sistema para certificar la autenticidad de copias digitales de documentos originales según realizaciones de la presente divulgación. El sistema de la presente divulgación está provisto de una aplicación 100 de cliente que se ejecuta en un dispositivo electrónico tal como un ordenador portátil, un teléfono móvil, una tableta y similares. El usuario opera la aplicación 100 de cliente a través de una Interfaz Gráfica de Usuario (GUI) para enviar documentos para su certificación. La aplicación 100 de cliente, en respuesta a recibir a través de la GUI una solicitud de usuario para certificar uno o más documentos originales, por ejemplo recibos de gastos basados en papel, escanea los documentos originales para obtener las copias digitales correspondientes. Por ejemplo, la aplicación 100 de cliente puede operar una cámara del dispositivo electrónico para obtener imágenes de

los documentos originales, que pueden almacenarse posteriormente en la memoria del dispositivo electrónico en el formato deseado, por ejemplo, JPG, PNG y similares. La aplicación 100 de cliente procesa las imágenes adquiridas en elementos de datos adicionales asociados con los documentos escaneados. Por ejemplo, en el caso de recibos de gastos, la aplicación 100 de cliente puede extraer elementos de datos asociados con los elementos de gastos, la cantidad correspondiente, la moneda, la fecha y la hora, la cantidad total pagada y similares. La aplicación 100 de cliente puede proporcionar además un conjunto de opciones al usuario para añadir información adicional asociada con los documentos originales que podrían usarse para la certificación. Una vez que la aplicación 100 de cliente recoge la información necesaria requerida para la certificación, que incluye las copias digitales de los documentos originales y los elementos de datos asociados con los documentos originales, prepara la información recogida para la certificación. Durante la etapa de preparación, cada copia digital de una página de un documento original se combina en un único documento electrónico de un formato digital deseado, tal como un formato de documento portátil (PDF), que posteriormente se firma digitalmente usando un algoritmo de hash criptográfico, por ejemplo SHA-256 o similar. Los elementos de datos correspondientes recogidos durante la solicitud de certificación se agrupan en una carga útil de datos. Los elementos de datos pueden extraerse del documento electrónico y/o proporcionarse por el usuario. La carga útil de datos contiene una gama de información tal como los elementos de datos asociados con los documentos originales, metadatos recopilados de la aplicación 100 de cliente, la firma digital generada del documento electrónico y similares. La aplicación 100 de cliente aplica una firma digital a la carga útil de datos, que se calcula en base a la información contenida en la misma y una clave compartida con el servidor 200 de certificación. Como resultado, cualquier cambio en la información contenida en la carga útil de datos provocaría un cambio en la firma digital. Para una protección adicional, la carga útil de datos puede enrollarse en un testigo de autenticación que se firma digitalmente usando una firma digital calculada basándose en la información contenida en la carga útil de datos y la clave criptográfica. El testigo de autenticación puede ser generado por un servicio de terceros. Como tal, la autenticación del testigo requeriría el conocimiento de la clave criptográfica correspondiente. El testigo criptográfico puede ser un testigo JSON Web o equivalente. La aplicación 100 de cliente transmite el documento electrónico firmado digitalmente y la carga útil de datos firmados digitalmente, que puede estar en forma de un testigo de autenticación, a un servidor 200 de certificación configurado para certificar las copias digitales de los documentos originales y los datos correspondientes. El servidor 200 de certificación está acoplado comunicativamente a una gama de servicios 300 de aplicación externos tales como sistemas de cliente externos. El servidor 200 de certificación está configurado para certificar la autenticidad de la información transmitida desde la aplicación de cliente y almacenar de forma segura la información autenticada.

La figura 2 muestra una arquitectura ejemplificada para el servidor 200 de certificación según realizaciones de la presente divulgación. El servidor 200 de certificación está provisto de un módulo 210 de comunicación configurado para facilitar el intercambio de datos entre las aplicaciones 100 de cliente que se ejecutan en dispositivos electrónicos de usuario correspondientes y/o la aplicación 300 de terceros. Por lo tanto, el módulo de comunicación está configurado para recibir la información transmitida desde la aplicación de cliente, que incluye el documento electrónico firmado digitalmente y la carga útil de datos, que puede estar en forma de un testigo de autenticación, como se explicó anteriormente. La información recibida en el módulo de comunicación es procesada por el módulo 210 de procesamiento de datos, donde la información contenida en la carga útil firmada digitalmente se extrae y la firma digital aplicada a la carga útil digital y/o el testigo de autenticación que contiene la carga útil digital se recalcula. La firma digital es recalculada por el módulo 230 de firma digital, que está provisto de los algoritmos criptográficos y claves criptográficas necesarios para duplicar el proceso de firma digital aplicado en la aplicación 100 de cliente. Como resultado, si los datos contenidos en la carga útil de datos han permanecido sin cambios, entonces la firma digital calculada por el módulo 230 de firma digital coincide con la aplicada por la aplicación de cliente. De lo contrario, si hay una diferencia entre la firma digital recalculada y la aplicada por la aplicación de cliente, el módulo 220 de procesamiento de datos considera que los datos en la carga útil de datos se han modificado posteriormente y por lo tanto no corresponden a los datos obtenidos de los documentos originales. Una vez que la carga útil de datos se ha autenticado, entonces el hash, también denominado firma digital, aplicado al documento electrónico por la aplicación de cliente y contenido en la carga útil de datos, se consideraría auténtico. Como tal, durante el procedimiento de autenticación en el servidor 200 de certificación, la firma digital del documento electrónico obtenido a partir de la carga útil de datos autenticados se compara por el módulo 220 de procesamiento de datos con la firma digital recalculada del documento electrónico firmado digitalmente transmitido por la aplicación 100 de cliente. De manera similar, al proceso de comparación aplicado a la carga útil de datos, si la firma digital del documento electrónico obtenida a partir de la carga útil de datos coincide con la firma digital recalculada, entonces el documento electrónico transmitido se considera auténtico. De lo contrario, si se identifica un desajuste, entonces el documento electrónico se ha manipulado y se rechaza del proceso de certificación. Como resultado, proporcionando un proceso de autenticación de dos etapas, donde la carga útil de datos se autentica primero y luego el documento electrónico, es posible identificar la modificación posterior que se produjo tanto en el documento electrónico como en la carga útil de datos. Una vez que las firmas digitales del documento electrónico y la carga útil de datos han sido autenticadas, el documento 111 electrónico es convertido a un formato deseado, por ejemplo, de PDF a PDF/A, y se aplica una firma digital al documento electrónico convertido. Posteriormente, el documento 232 electrónico convertido y la carga útil de datos, o parte de la información contenida en la carga útil de datos, se almacenan en una parte de la base 240 de datos fiable asociada con el usuario y/u organización de usuario vinculada a la aplicación 100 de cliente. La base 240 de datos fiable devolvería un número de identificación de referencia y una marca de tiempo para el registro generado, que puede reenviarse a la aplicación de cliente y/o al servicio de terceros.

La figura 3 muestra una implementación ejemplificada del sistema de la figura 1 para certificar la autenticidad de copias digitales y los datos correspondientes asociados con recibos de gastos basados en papel según realizaciones de la presente divulgación. Una aplicación 100 de cliente que se ejecuta en un dispositivo electrónico de un usuario es utilizada por el usuario para digitalizar los recibos de gastos originales y los datos acompañados. La aplicación 100 de cliente, a petición del usuario, crea un documento 111 PDF vacío que contendría imágenes de los recibos de gastos escaneados. Una vez que se abre el documento 111 PDF, la aplicación 100 de cliente obtiene imágenes de los recibos de gastos usando una cámara del dispositivo electrónico, por ejemplo, la cámara telefónica integrada. La aplicación 100 de cliente procesa cada imagen obtenida ejecutando un algoritmo de detección de fotograma en la fotografía tomada para generar una página de documento que se añadirá al documento 111 PDF. La aplicación 100 de cliente, en base a los resultados del algoritmo de detección de fotogramas, extrae y elimina distorsiones de la página de documento y presenta la página de documento procesada al usuario para su aprobación para garantizar la exactitud, nitidez y legibilidad del documento. Tras la aprobación del usuario, la aplicación 100 de cliente añade la página de documento generada al documento 111 PDF. Se genera una nueva página de documento para cada página del recibo original y se añade al documento PDF, siguiendo el mismo procedimiento que el descrito anteriormente. La aplicación 100 de cliente presenta además al usuario un formulario o un menú para añadir datos adicionales para homologación fiscal, tales como información personal, código fiscal y similares. Además, la aplicación 100 de cliente puede extraer datos de las imágenes asociadas con los recibos de gastos, tales como la cantidad para cada artículo comprado, hora y fecha, país, número de factura y similares. Se solicita al usuario que proporcione el consentimiento de la información asociada con los recibos de gastos y homologación fiscal para asegurar la exactitud de la información recogida. Una vez que el usuario aprueba la exactitud de la información, la aplicación de cliente firma digitalmente el documento PDF calculando un valor de hash único usando un algoritmo de función hash conocido tal como SHA-256 o similar. Además del documento 111 PDF, la aplicación 100 de cliente prepara una carga útil de datos a cargar que contiene, entre otros, los datos recogidos del usuario y las imágenes y el valor hash del documento 111 PDF. Como se muestra en la figura 3, la extracción de datos y la homologación de impuestos se pueden realizar en los lados del servidor 200 de certificación usando respectivamente el sistema 221 correspondiente y un módulo 221 lector de imágenes, que puede ser parte del módulo 220 de procesamiento del servidor 200 de certificación. La aplicación 100 de cliente crea un testigo 112 web JSON correspondiente que contiene la carga útil de datos y una firma digital calculada en base a la carga útil de datos y una clave criptográfica compartida entre la aplicación 100 de cliente y el servidor 200 de certificación. La aplicación 100 de cliente carga el documento PDF firmado digitalmente y el testigo Web JSON en una pasarela 211 de comunicación, que es parte del módulo 210 de comunicación del servidor 200 de certificación.

La pasarela 211 de comunicación recibe la solicitud de carga desde la aplicación de cliente, que contiene el documento 111 PDF y el testigo 112 Web JSON (JWT). En la pasarela 211 de comunicación, el JWT se valida volviendo a calcular la firma digital en función de la carga útil recibida y la clave criptográfica compartida. Si la firma recalculada coincide con la firma digital del JWT cargado, entonces el JWT 112 se considera intacto y la información contenida en el mismo es auténtica. El JWT 112 validado se reenvía, junto con el documento 111 PDF, al servicio 231 de firma, que es parte del módulo 230 de firma digital, para su validación. El servicio 231 de firma recibe la solicitud de carga desde la pasarela 211 de comunicación que contiene el documento 111 PDF y el JWT 112. Como la validez del JWT 112 ya ha sido comprobada por la pasarela 211 de comunicación, el servicio 231 de firma considera que la información contenida en el mismo es también auténtica. Como tal, el servicio 231 de firma digital extrae el hash del archivo 111 de documento PDF del JWT 112 y lo compara con un hash recalculado del documento 111 PDF cargado. Si las firmas coinciden, entonces el documento 111 PDF cargado se considera auténtico, es decir, no se detectan modificaciones posteriores al procesamiento. Si la firma no coincide, entonces el documento PDF es rechazado, y se emite una alerta que indica que el documento PDF no es válido. El mismo proceso sigue la pasarela 211 de comunicación cuando se detecta un JWT 112 no válido. El documento 111 PDF validado se convierte del formato PDF a formato PDF/A-3U o similar. En el servicio 231 de firma, la información adicional puede añadirse al documento PDF/A convertido, que incluye información de metadatos tal como fecha de captura, nombre de software, versión de software, código de homologación de impuestos, y similares. El documento PDF/A se firma digitalmente aplicando un certificado de autenticación digital de una base de datos de certificación. El servicio 231 de firma digital puede validar el estado del certificado de autenticación digital seleccionado entrando en contacto con un servicio 310 de certificación externo. Si el certificado es válido, entonces el documento PDF/A firmado se valida contra el estándar 3U de PDF/A para cumplimiento. Si el certificado no es válido, entonces se selecciona un nuevo certificado de la base de datos de certificación. En general, la base de datos de certificación puede comprender una o más certificaciones de autenticación, que pueden precargarse y/o refrescarse a intervalos regulares. El documento 232 PDF/A validado y los datos de gastos anotados se cargan en una base 240 de datos fiable para su almacenamiento. En respuesta, la base 240 de datos fiable genera un registro de datos_ID del documento PDF (por ejemplo, factura_ID), un id recepción y una marca de tiempo de inserción. El servicio 231 de firma digital, en respuesta a la recepción de la información de la base de datos fiable, extrae una imagen de la primera página del archivo PDF/A y la carga en un módulo 233 de gastos, junto con los valores tomados de los datos de gasto anotados, utilizando la información de cuenta del cliente contenida en el JWT 112.

La base 240 de datos fiable, en respuesta a recibir una solicitud para cargar un documento 232 PDF/A y datos de gastos anotados, recupera la última entrada en una tabla, por ejemplo, división de la tabla asociada con el usuario. La base 240 de datos fiable inserta una nueva entrada en recepción_id incrementado, un hash del archivo PDF firmado y un hash de los datos de gastos. La base de datos fiable comprueba el número de identificación única (ID), por ejemplo factura_ID, añadido al archivo PDF, y si ya existe en la tabla, no crea una nueva entrada en la tabla sino que

más bien devuelve el número de identificación de registro de datos (ID) existente (factura_id), recepción_id y marca de tiempo del servicio 231 de firma. Si no existe el ID único, entonces la base de datos fiable inserta el documento 232 PDF/A como un nuevo archivo, vinculado a la factura usando la firma digital del documento PDF/A, e inserta los datos de gastos anotados en la tabla de gastos, vinculados a la factura_id, y el hash de esta entrada inicial de datos_de_coste. Junto con el elemento de gasto, se almacena un valor aleatorio. La base de datos fiable devuelve el valor de factura_id único global al servicio 231 de firma, junto con recepción_id (que es solo único para el sistema) y la marca de tiempo de inserción.

La base 240 de datos fiable almacena los documentos 231 PDF/A firmados junto con los datos de gastos anotados. Además, el servicio 240 de DB fiable escribe una cadena hash que contiene todas las facturas registradas por su representación firmada PDF/A y los datos de gastos para probar la validez e integridad de los recibos almacenados. Además, es responsable de cerrar la corriente y crear nuevos periodos de contabilidad para cada cliente basándose en la configuración del cliente. Cada periodo de contabilidad debe estar cerrado por una firma que contenga la función hash de comienzo y final de ese periodo de contabilidad. El mismo certificado, que se usa para firmar archivos PDF/A, también se usa para crear la firma de cierre usando el servicio 231 de firma (SIG) para firmar el cierre de periodo.

La figura 4 muestra una cadena 242 de hash representativa creada en la base 240 de datos fiable para registrar transacciones en bloques 243_1-243_n de datos hash únicos. Durante una fase de inicialización, se genera un primer registro 247_1 de datos que comprende la firma 244 digital del documento electrónico y la firma 245 digital de JSON. Las firmas 244 y 245 digitales pueden estar en forma de un código hash. Al registro 247_1 digital se le asigna un número de identificación de referencia 247 "recepción_1, que se incrementa para registros 247_1-n de datos posteriores. Basándose en las firmas 244 y 245 digitales contenidas en el registro 247_1 de datos, se genera un bloque 243_1 de datos en la cadena 242 de hash, al que se le asigna un código 246_1 de hash único. El código 246_1 hash del primer bloque 243_1 de datos se genera basándose al menos en el código 244 hash del documento electrónico y el código 245 hash de JSON. Para bloques 243_n de datos posteriores correspondientes a nuevos registros 247_n de datos, el código 246_1-246_n hash único de cada bloque 243_1-243_n hash puede basarse además en el código 246_n-1 hash de un bloque 243_n-1 de datos anterior, asegurando de ese modo que un nuevo bloque de datos esté vinculado al bloque de datos anterior. Los bloques 243_1-n de datos generados durante un periodo cronológico específico, por ejemplo un periodo de contabilidad, pueden representar recibos de datos individuales enviados por un usuario o usuarios correspondientes durante un periodo de tiempo. Un servicio 240 de base de datos fiable puede usarse para cerrar la corriente y crear nuevos periodos cronológicos, por ejemplo periodos de contabilidad, para cada cliente y sus usuarios correspondientes en base a la configuración del cliente. Cada periodo de contabilidad puede cerrarse mediante una firma 249a generada basándose en la primera firma 246_1 digital y la última firma 246_n digital aplicadas al primer y último bloque 243-1-n de datos del periodo de contabilidad especificado. La firma 249a de cierre se usa para verificar las transacciones producidas durante el periodo especificado, sin la necesidad de procesar por separado la información almacenada en cada registro 247_1-n de datos. La firma 249a de cierre puede firmarse usando el certificado usado por el servicio 231 de firma.

En general, el módulo 212 lector de gastos está provisto de un algoritmo de detección de fotogramas que usa una red neuronal convolucional (CNN) autoentrenada para detectar y procesar los documentos originales enviados para escaneado. El resultado de la detección de fotogramas se usa para recortar y des-distorsionar la parte de las imágenes captadas que muestra el documento original basado en papel. Para evitar la edición de fotogramas, la aplicación 100 de cliente evita la interacción humana durante el proceso de escaneo. La aplicación 100 de cliente evita además que los usuarios tomen imágenes que contienen múltiples facturas o múltiples páginas de una única factura al mismo tiempo, por ejemplo imágenes que muestran múltiples recibos de gastos. Para este propósito, el módulo 211 lector de gastos puede usar una pequeña red neuronal entrenada para detectar si hay múltiples recibos mostrados dentro del alcance de la cámara y evitar que los usuarios tomen fotos. Debe observarse que aunque el módulo 212 lector de gastos se muestra como parte del servidor 200 de certificación, puede ser igualmente parte de la aplicación 110 de cliente que se ejecuta en el dispositivo electrónico.

El módulo 212 lector de gastos puede usar imágenes de mapas de bits, por ejemplo JPEG, como formato de imagen de entrada para PDF. La adición de imágenes de mapas de bits en PDF no incorpora la imagen de entrada (por ejemplo, PNG, GIF, JPEG, JPEG2K, etc.), sino que la imagen de entrada se transforma para dar una codificación interna soportada por filtros internos definidos por el estándar de PDF. Por ejemplo, la decodificación DCT es una implementación bastante próxima del estándar JPEG, pero no cumple necesariamente con el estándar JPEG. Transformando las imágenes a un formato de codificación interno se asegura que el documento PDF pueda visualizar el contenido de una imagen, incluso cuando la implementación interna y el estándar oficial divergen en el futuro.

En general, el protocolo 310 de estado de certificado en línea (OCSP) es un servicio proporcionado por un proveedor de terceros para comprobar la validez de un certificado de autenticación. El servicio 231 de firma digital, o la base 240 de datos fiable, u otro servicio encargado de aplicar un certificado de autenticación puede generar una solicitud a los proveedores de terceros para comprobar la validez del certificado usando el enlace URL incluido en el certificado. El servicio 310 OCSP puede estar dispuesto para proporcionar, por adelantado, alertas relacionadas con la invalidación y/o revocación de un certificado que puede almacenarse en la memoria caché. Los resultados de una solicitud generada por el servidor de certificación al OCSP 310 pueden considerarse válidos durante un cierto periodo, por ejemplo, 2 días. Con el fin de reducir la carga de red y garantizar que un fallo de conectividad no interfiera con el proceso de firma, las respuestas de OCSP pueden almacenarse en caché durante un marco de tiempo predefinido,

que puede ser más corto que la validez del certificado, por ejemplo, durante 6 horas. Después de este tiempo, las respuestas OCSP almacenadas en caché pueden refrescarse. Si la actualización falla debido a problemas de conectividad, todavía hay tiempo para arreglar el problema de conectividad o reemplazar el certificado, por ejemplo, obtener uno nuevo.

5 El servicio 231 de firma contiene un conjunto de certificados de firma almacenados en una base de datos de certificación de la que se elige el certificado activo. La fecha de caducidad del certificado activo y el estado de revocación almacenado en caché se comprueban antes de aplicar una firma digital. Si la respuesta del OCSP 310 indica que el certificado fue revocado o que el certificado ha expirado, el certificado se elimina del conjunto de certificados y toma el siguiente certificado. Se pueden emitir nuevos certificados para refrescar el conjunto de
10 certificados.

Un método 500 ejemplificado para certificar copias digitales de documentos originales se presenta en la figura 5. El proceso comienza recibiendo en la aplicación 100 de cliente una solicitud de certificación digital de documentos originales, por ejemplo recibos de gastos. La aplicación 100 de cliente, en la etapa 510, adquiere copias digitales de los documentos originales a certificar y elementos de datos correspondientes asociados con los documentos
15 originales. Por ejemplo, como se ha explicado anteriormente, las imágenes de los documentos originales pueden obtenerse usando la cámara del dispositivo electrónico del usuario. En la etapa 520, la aplicación 100 de cliente genera un documento 111 electrónico de un primer formato digital, por ejemplo, PDF, que contiene las imágenes adquiridas, y una carga 112 útil de datos que comprende los elementos de datos asociados con cada documento original. El documento 111 PDF y la carga útil de datos se firman digitalmente, en la etapa 530, calculando las firmas digitales
20 respectivas. La firma digital del documento 111 electrónico se añade a los datos contenidos en la carga útil de datos. La aplicación 100 de cliente comunica, en la etapa 530, el documento 111 PDF firmado y la carga 112 útil de datos, que puede estar en forma de un testigo Web JSON. En la etapa 540, la carga 112 útil de datos cargada y los documentos 111 PDF se reciben en el servidor 200 de certificación, donde se procesan para determinar su autenticidad, como se explicó anteriormente. Una vez que se ha verificado su autenticidad, en la etapa 550, se aplica
25 una certificación de autenticación, como se ha descrito anteriormente, por el servicio 231 de firma. El documento 111 PDF de autenticación y la carga 112 útil de datos se almacenan en una base 240 de datos fiable, en la etapa 560, generando un registro de datos que comprende el documento electrónico autenticado y elementos de datos asociados obtenidos de la carga útil de datos autenticados. En respuesta a la generación del registro de datos, la base de datos fiable devuelve un número de identificación único y una marca de tiempo asociada con la generación del registro de
30 datos.

En algunas realizaciones, el método comprende etapas de método correspondientes a cualquiera de los sistemas para gestionar la asignación de funciones de recursos informáticos expuestas anteriormente.

REIVINDICACIONES

1. Un método para certificar la autenticidad de copias digitales de documentos originales en un servidor (200) de certificación de datos, comprendiendo el método:

5 recibir, de una aplicación (100) de cliente que se ejecuta en un dispositivo electrónico de un usuario, una carga (112) útil de datos firmados digitalmente y un documento (111) electrónico firmado digitalmente correspondiente asociado con un documento original,

en donde el documento (111) electrónico firmado digitalmente comprende una copia (113) digital de un documento original que contiene una o más páginas y una firma digital generada del documento (111) electrónico,

10 en donde la carga (112) útil de datos firmados digitalmente comprende la firma digital del documento (111) electrónico, elementos de datos asociados con el documento original, y una firma digital generada de la carga (112) útil de datos calculada en base a la firma digital del documento (111) electrónico y los elementos de datos asociados con el documento original; y

certificar y almacenar la carga (112) útil de datos firmados digitalmente recibidos y el documento (111) electrónico firmado digitalmente correspondiente realizando las etapas:

15 recalcular las firmas digitales correspondientes para la carga (112) útil de datos firmados digitalmente y el documento (111) electrónico y comparar las firmas recalculadas con las firmas digitales del documento (111) electrónico y la carga (112) útil de datos aplicada en la aplicación (100) de cliente; y

en respuesta a la determinación de la coincidencia de las firmas digitales del documento electrónico y de la carga útil de datos:

20 autenticar el documento (111) electrónico y la carga (112) útil de datos correspondiente aplicando un certificado de autenticación, que se recupera de una base de datos de certificación del servidor de certificación;

generar, en una parte de una base (240) de datos fiable asociada con el usuario y/u organización de usuario vinculada a la aplicación (100) de cliente, un registro (247_1-n) de datos que comprende el documento electrónico autenticado y elementos de datos asociados obtenidos a partir de la carga útil de datos autenticados; y

25 devolver un número (247) de identificación único y una marca de tiempo asociada a la generación del registro (247_1-n) de datos.

30 2. El método según la reivindicación 1, en donde la etapa de generar un registro de datos comprende la etapa de generar un nuevo bloque de datos en un libro de registro digital de la base de datos fiable asociada con el usuario y/u organización de usuario a la que está vinculada la aplicación de cliente, estando cada bloque de datos del libro de registro digital dispuesto en orden cronológico según la información de la marca de tiempo del registro de datos correspondiente.

3. El método según la reivindicación 2, en donde a cada bloque de datos en el libro de registro digital se le asigna una firma digital única calculada basándose en al menos las firmas digitales del documento electrónico y la carga útil de datos.

35 4. El método según cualquiera de las reivindicaciones 2 o 3, en donde el servidor de certificación está configurado para autenticar la información contenida en los bloques de datos creados en el libro de registro digital asociado con el usuario a lo largo de un marco de tiempo especificado realizando las etapas de:

recuperar, en base al orden cronológico de bloques de datos, la firma digital única del primer y último bloque de datos en el libro de registro digital asociado con el marco de tiempo especificado;

40 calcular, basándose en firmas digitales recuperadas, una firma de cierre para el marco de tiempo especificado; y

aplicar un certificado de autenticación a la firma de cierre calculada, que se recupera de la base de datos de certificación.

5. El método según cualquiera de las reivindicaciones anteriores, en donde la etapa de aplicar el certificado de autenticación al documento electrónico autenticado comprende las etapas de:

45 convertir el documento electrónico autenticado de un primer formato digital a un segundo formato digital predefinido; añadir metadatos al documento electrónico convertido; y

aplicar al documento electrónico convertido el certificado de autenticación recuperado.

6. El método según cualquiera de las reivindicaciones anteriores, en donde la etapa de recuperar un certificado de autenticación de la base de datos de certificación comprende las etapas de:

5 comprobar la validez del certificado de autenticación seleccionado emitiendo, a través de un enlace incluido en cada certificado de autenticación, una solicitud a un servicio de certificación para comprobar la validez y/o el estado de revocación del certificado de autenticación seleccionado;

en donde si la respuesta recibida del servicio de certificación indica que el certificado seleccionado es inválido y/o revocado, el servidor de certificación está configurado para realizar las etapas de:

eliminar el certificado no válido de la base de datos de certificados;

seleccionar un nuevo certificado de autenticación de la base de datos de certificados; y

10 comprobar la validez del nuevo certificado de autenticación.

7. El método según cualquiera de las reivindicaciones anteriores, en donde la etapa de determinar la autenticidad del documento electrónico y la carga útil de datos comprende las etapas de:

15 recalcular la firma digital aplicada a la carga útil de datos en función de los datos contenidos en la carga útil de datos y de una clave criptográfica compartida, y comparar la firma digital recalculada con la firma digital de la carga útil de datos;

en respuesta a la determinación de que la firma recalculada es igual a la firma digital de la carga útil de datos, extraer de la carga útil de datos validada el valor hash del documento electrónico; y

comparar el valor hash extraído de la carga útil de datos validada con el valor hash recalculado del documento electrónico firmado recibido en el servidor de certificación.

20 8. El método según cualquiera de las reivindicaciones anteriores, en donde la etapa de devolver un número de identificación único y una marca de tiempo asociada con la generación del registro de datos comprende la etapa de comunicar una copia del registro de datos a una o más aplicaciones de cliente conectadas.

9. Un sistema para certificar la autenticidad de copias digitales de documentos originales, comprendiendo el sistema:

25 una aplicación (100) de cliente que se ejecuta en un dispositivo electrónico de un usuario configurada, en respuesta a la recepción de una solicitud de certificación de un usuario para certificar una copia digital de un documento original, para

adquirir una copia digital de cada página del documento original a certificar y los elementos de datos correspondientes,

30 generar un documento electrónico de un primer formato digital que contiene las copias digitales adquiridas asociadas a las páginas del documento original y una carga útil de datos que comprende los elementos de datos asociados al documento original,

firmar digitalmente la carga útil de datos y el documento electrónico calculando una firma digital correspondiente para la carga útil de datos y el documento electrónico, en donde la firma digital del documento electrónico se añade a los datos contenidos en la carga útil de datos antes de la firma, y

35 comunicar la carga útil de datos firmados y el documento electrónico firmado al servidor de certificación de datos; y

un servidor (200) de certificación acoplado comunicativamente a la aplicación de cliente configurado, en respuesta a la recepción de la carga útil de datos firmados y el documento electrónico firmado, para realizar las etapas del método según las reivindicaciones 1 a 8.

40 10. El sistema según la reivindicación 9, en donde la aplicación (100) de cliente está configurada para firmar digitalmente la carga útil de datos al envolver la carga útil de datos en un testigo de autenticación, comprendiendo el testigo de autenticación una firma calculada en base a los datos contenidos en la carga útil de datos y una clave criptográfica compartida entre la aplicación de cliente y el servidor de certificación.

45 11. El sistema según la reivindicación 10, en donde la aplicación de cliente está configurada para firmar digitalmente la carga útil de datos calculando adicionalmente un hash para el documento electrónico usando una función hash.

12. El sistema según cualquiera de las reivindicaciones 9 a 11, en donde los documentos originales y las copias digitales correspondientes están en forma de recibos de gastos basados en papel que comprenden información de gastos.

13. El sistema según cualquiera de las reivindicaciones 9 a 12, en donde la base de datos fiable del servidor de certificación está dividida en una pluralidad de partes, cada una asociada con un usuario y/u organización de usuario vinculada con la aplicación de cliente.
- 5 14. El sistema según la reivindicación 13, en donde el servidor de certificación está configurado para identificar, basándose en la información transmitida desde la aplicación de cliente, la identidad del usuario y/u organización del usuario y, en consecuencia, dirigir datos a la parte correspondiente de la base de datos fiable.
- 10 15. Un producto de programa informático que comprende instrucciones de código de programa almacenadas en un medio legible por ordenador, que cuando se ejecutan por un módulo procesador de un servidor de certificación en respuesta a la recepción de una solicitud de una aplicación de cliente para certificar una carga útil de datos firmados y un documento electrónico firmado, hacen que el servidor de certificación realice las etapas del método según cualquiera de las reivindicaciones 1 a 8.

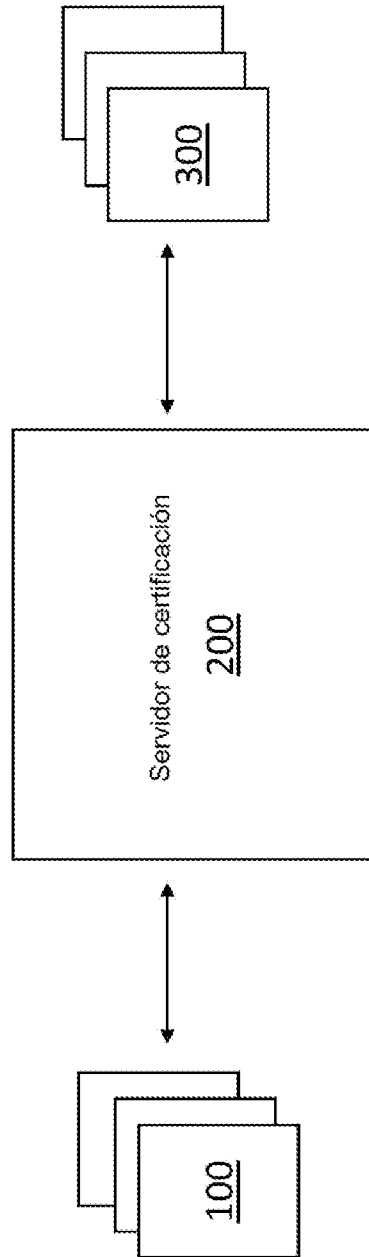


Figura 1

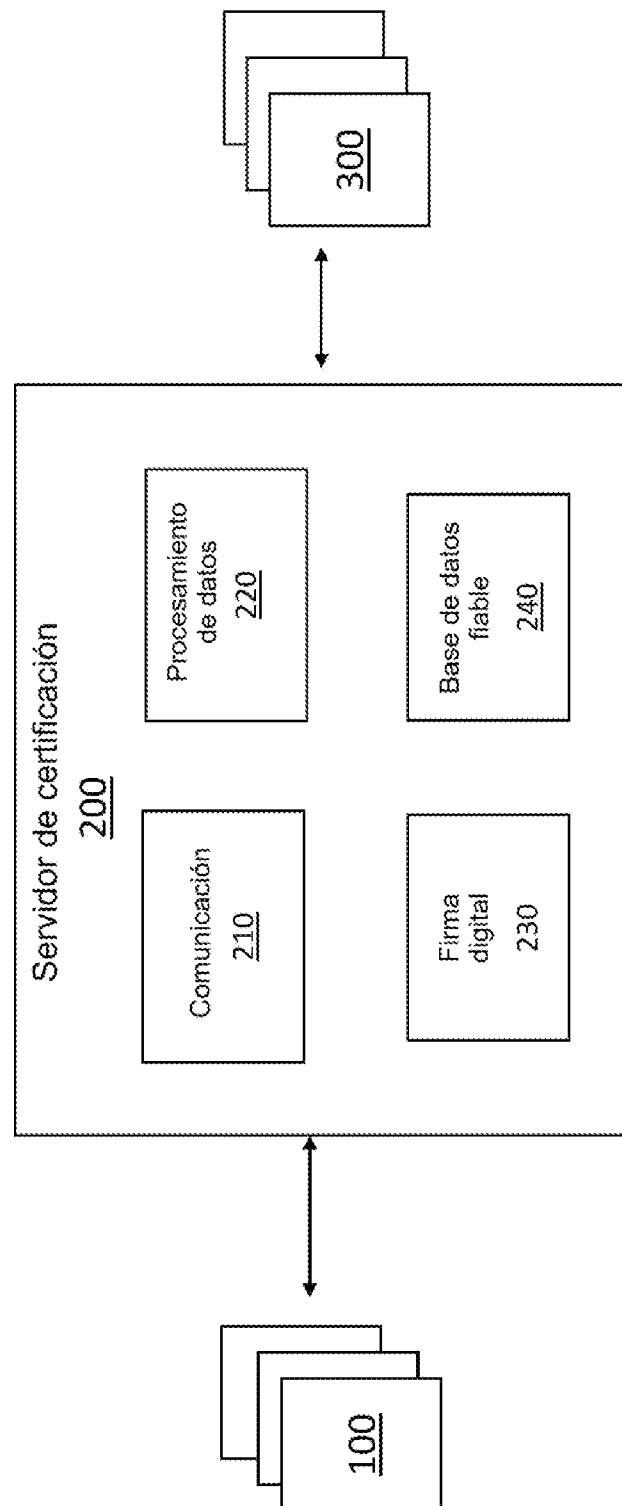


Figura 2

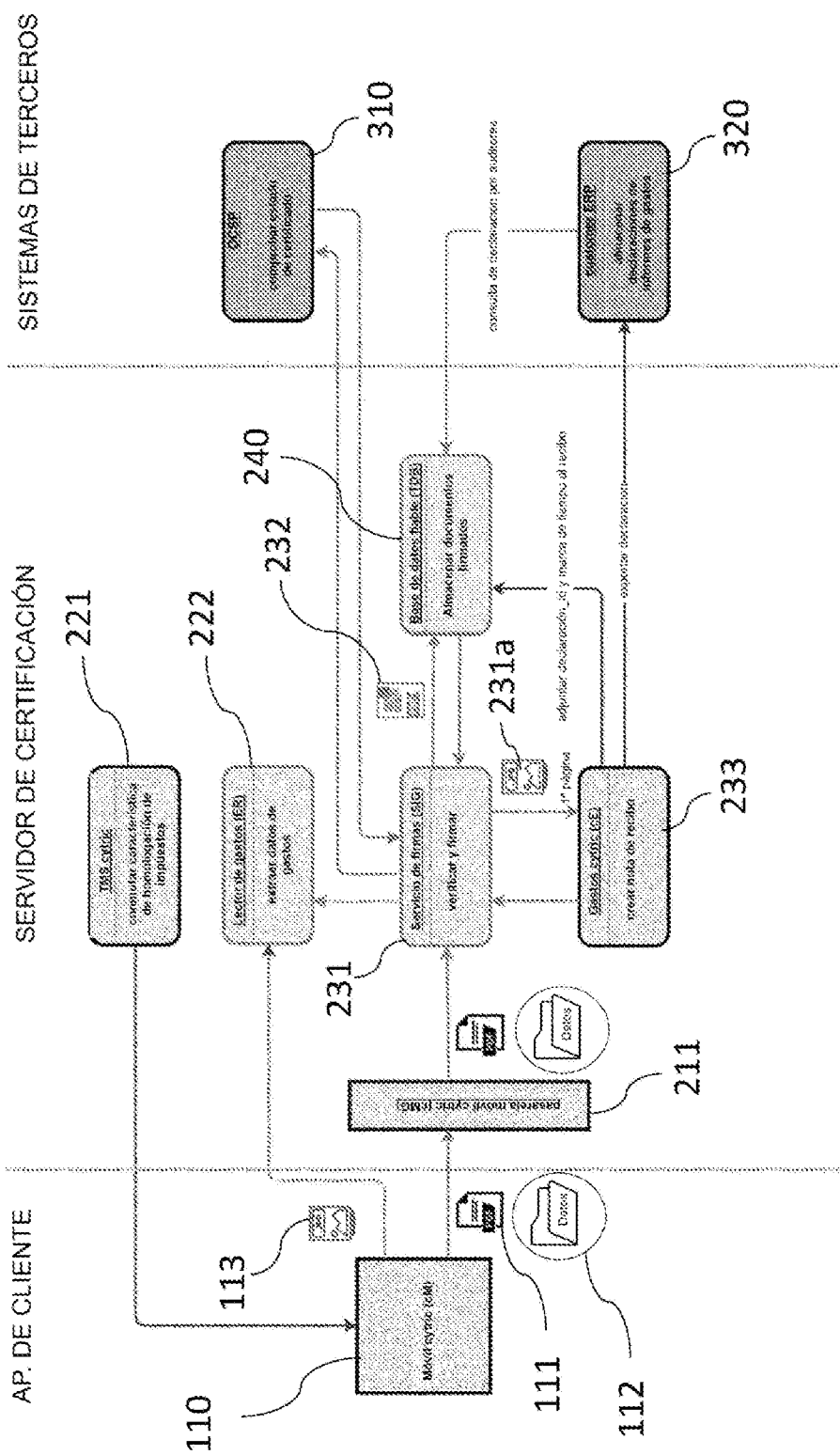


Figura 3

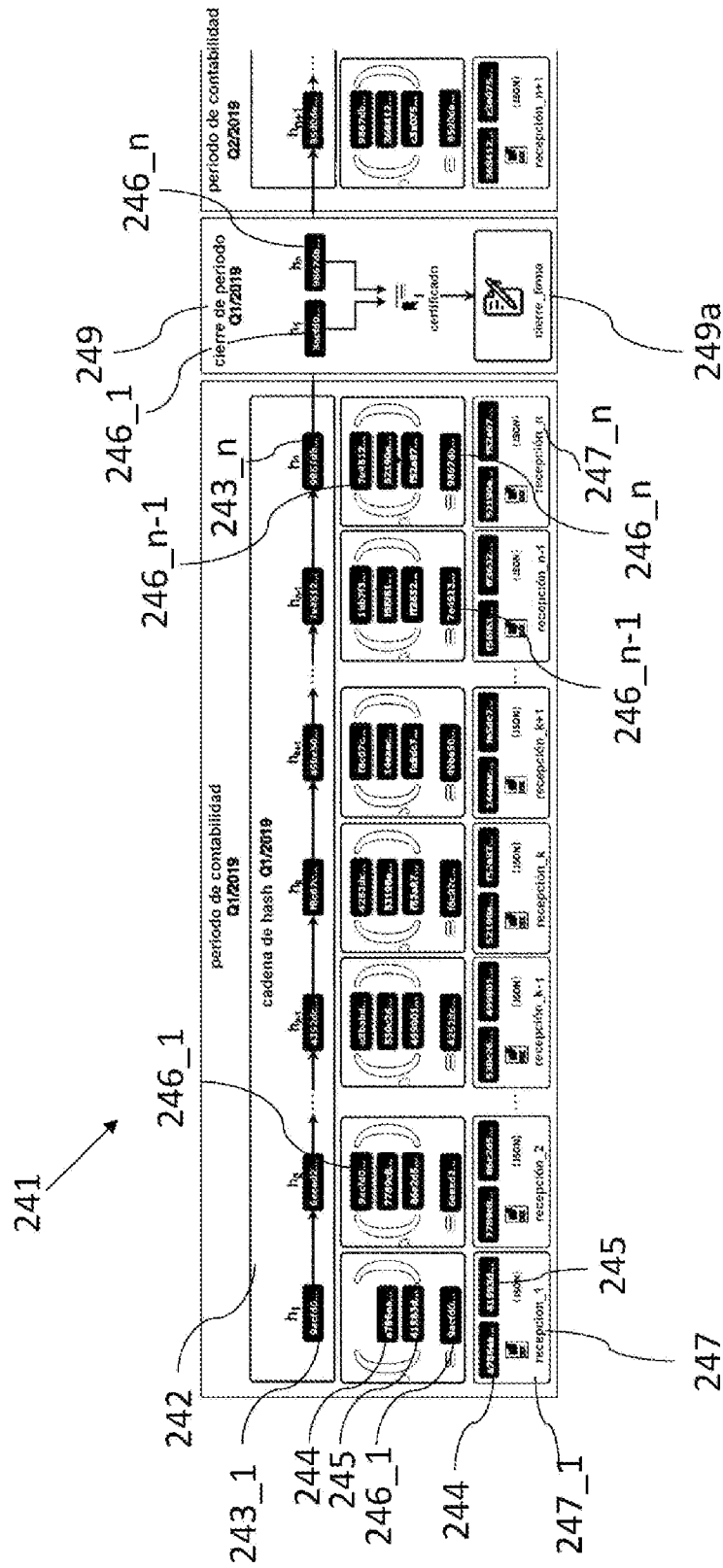


Figura 4

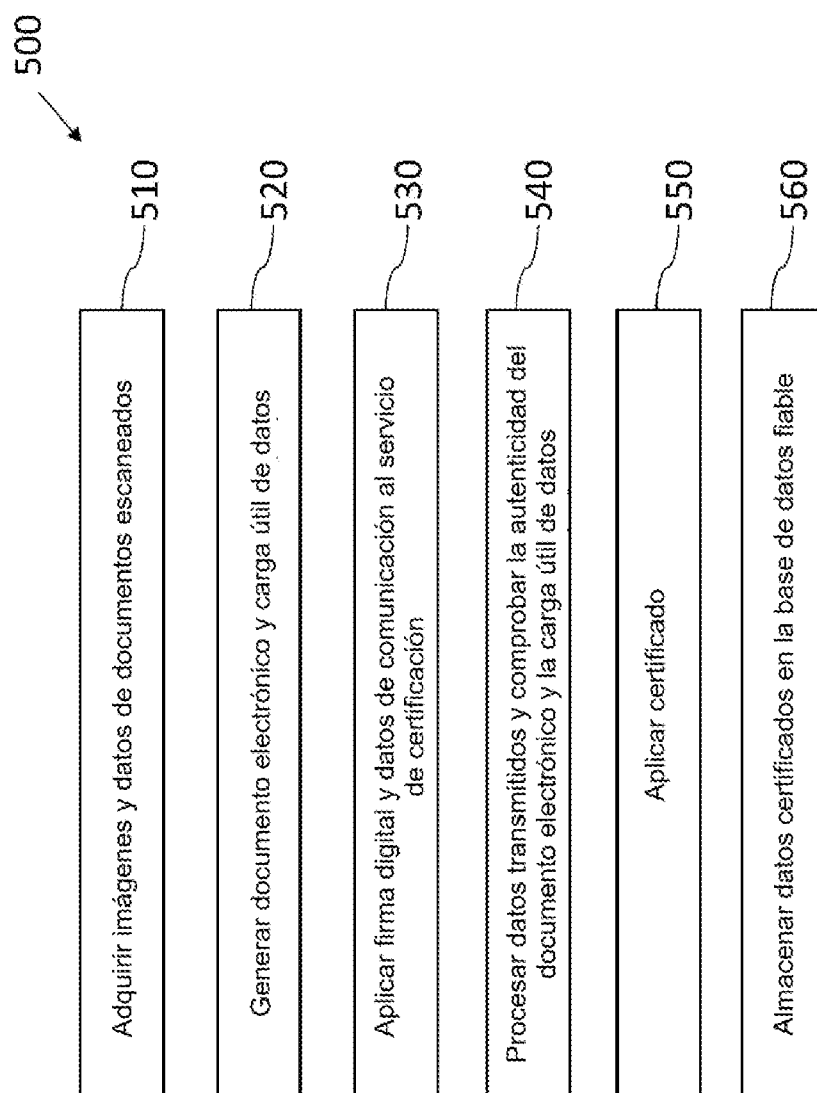


Figura 5