(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 631 078**

(51) Int. CI.:

H04L 12/58 (2006.01)
G06Q 10/10 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.02.2012 E 12382060 (7)**

(97) Fecha y número de publicación de la concesión europea: **08.03.2017 EP 2632096**

(54) Título: **Método para la certificación del envío de mensajes electrónicos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.08.2017

(73) Titular/es:

LLEIDANETWORKS SERVEIS TELEMÀTICS S.A. (100.0%)
Parque Tecnológico Agroalimentario, Edificio H1, 2ª planta
25003 Lleida, ES

(72) Inventor/es:

SAPENA SOLER, FRANCISCO

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Método para la certificación del envío de mensajes electrónicos

OBJETO DE LA INVENCIÓN

El objeto de la invención es un método para que un operador de telecomunicaciones pueda recibir, reenviar y enviar correo electrónico de un usuario emisor a uno o a varios destinatarios, registrándose todas las operaciones transaccionales para, finalmente, firmarlo digitalmente y entregar al usuario emisor un certificado como operador y tercera parte de confianza.

ANTECEDENTES DE LA INVENCIÓN

Se sabe que, actualmente, las comunicaciones electrónicas se han convertido en una herramienta esencial e indispensable para cualquier operativa, tanto legal como ilegal. Las comunicaciones se utilizan para todo tipo de transacciones, generación de llamadas y mensajes, etc., de un origen a un destino.

Las operadoras de telecomunicaciones son las que proporcionan las infraestructuras que gestionan, dirigen y almacenan gran parte de este tráfico. Estas operadoras de telecomunicaciones están sujetas a normativas, entre otras cosas, para la utilización del espectro radioeléctrico, que es limitado, o para la utilización de recursos de numeración telefónica, que también son finitos.

Las operadoras de telecomunicaciones, además, mantienen registros de las transacciones que realizan los usuarios con los objetivos, entre otros, de tarificación, registro de los números asociados a los mismos, referencias de facturación, así como el registro de cualquier dato transaccional utilizado en la facturación al usuario. Estos registros son conservados para posteriores verificaciones de tarificación y/o seguimiento del tráfico por parte del usuario.

En ocasiones, las autoridades judiciales solicitan a las operadoras de telecomunicaciones datos registrados de las transacciones electrónicas efectuadas, ya que las consideran terceras partes de confianza a efectos de proporcionar estos datos, así como cualquier dato que pueda ayudar a determinar las personas físicas o jurídicas que han efectuado el acto en cuestión.

Sin embargo, la búsqueda de los datos solicitados a la operadora de telecomunicaciones es normalmente complicada ya que se realiza en registros de actividades de gran volumen, normalmente diseñados para la facturación más que para el seguimiento de la trazabilidad de los datos. Por lo tanto, la búsqueda antes mencionada de los datos solicitados puede consumir una cantidad ingente de recursos de la operadora de telecomunicaciones.

Una vez localizados los datos solicitados por las autoridades judiciales, el operador emite un certificado en el que manifiesta explícitamente los datos transaccionales solicitados, la frecuencia, los destinos, así como cualquier información que haya solicitado la autoridad judicial pertinente.

Igualmente, existe en los usuarios esta misma necesidad de disponer de la capacidad de solicitar esta información a las operadoras de telecomunicaciones con el objeto de conocer y certificar los propios datos transaccionales, por ejemplo, los datos transmitidos, la fecha, los datos de recepción o cualquier otra información útil para el usuario. Esta necesidad puede venir motivada por la petición de una tercera parte al usuario de los datos transaccionales antes mencionados.

En el estado actual de la técnica se conocen diversos métodos y sistemas para la verificación de la transmisión así como de la integridad de los datos contenidos en un correo electrónico. Estos métodos conocidos normalmente proporcionan pruebas y contenidos del envío y recepción de correos electrónicos basándose en una solución tecnológica que permite verificar la transmisión.

Sin embargo, los métodos conocidos en el estado actual de la técnica poseen la desventaja de que implementan algoritmos y verificaciones que modifican el contenido del mensaje y además precisan comparar la firma digital del documento generado con la firma digital almacenada en el servidor. Estas verificaciones son electrónicas y se realizan en línea, lo que puede ser una desventaja para algunas terceras partes que solicitan este servicio.

Para ello, en caso de que un usuario emisor desee certificar un mensaje de correo electrónico, el mensaje pasa, en vez de por la ruta tradicional para su envío al destinatario, por una segunda ruta que implica el envío del mensaje al destinatario a través del servidor de una entidad certificadora. Sin embargo, esto supone una desventaja ya que el

mensaje es manipulado en este envío a través del servidor de la entidad certificadora, por lo que el mensaje finalmente recibido por el destinatario no es realmente el original enviado por el emisor, sino el transformado por la entidad certificadora.

Además de lo anterior, los métodos conocidos en el estado actual de la técnica archivan un algoritmo criptográfico único asociado a cada mensaje, es decir, la firma digital. Posteriormente, en caso de querer verificar el mensaje hay que comparar la firma digital de un documento generado con la firma digital guardada en el servidor de la entidad certificadora teniendo de nuevo que realizar un algoritmo de comparación entre el algoritmo criptográfico, que es el dato que genera y guarda el sistema conocido del estado actual de la técnica, y la anterior comparación debe llevarse a cabo haciendo uso de un algoritmo de comparación.

Como caso especial en el que se necesita demostración de la entrega al destinatario, está la recepción de las facturas emitidas por un usuario generador para poder demostrar así que posteriormente a la recepción de las prestaciones de servicios o productos, un usuario destinatario ha recibido la factura de esos servicios, evitando así que los usuarios destinatarios de un producto o servicio aleguen la no recepción de la correspondiente factura para evitar o retrasar el pago de la misma.

Los métodos conocidos en el estado actual de la técnica de notificación oficial, tales como el telegrama, el burofax o la carta certificada tienen varias desventajas como son la no mecanización del proceso, lo que revierte en un elevado consumo de tiempo así como un alto coste. Por ejemplo, el documento US2007174402 describe un sistema y un procedimiento para verificar la entrega y la integridad de correos electrónicos, donde un servidor transmite un mensaje desde un emisor a una dirección de destino. Durante la transmisión, el servidor y la dirección de destino mantienen un diálogo que constituye un elemento adjunto, a través de un protocolo particular, ya sea SMTP o ESMTP, referente al mensaje, al servidor y la dirección de destino. El mensaje pasa por servidores dispuestos entre el servidor y la dirección de destino. Esta ruta se incluye en el elemento adjunto. Se proporcionan verificadores para el mensaje y para los elementos adjuntos. Los verificadores pueden constituir datos *hash* cifrados del mensaje y del elemento adjunto. El emisor recibe el mensaje, los elementos adjuntos y las verificaciones desde el servidor antes de la autenticación y transmite el mensaje, los elementos adjuntos y los verificadores al servidor para obtener autenticación mediante el servidor. El servidor actúa sobre el mensaje y el verificador del mensaje para autenticar el mensaje y actúa sobre los elementos adjuntos y el verificador de los elementos adjuntos para verificar los elementos adjuntos. En el documento US2008278740 se describe un procedimiento, un sistema y un producto de programa informático para la comunicación masiva de información a destinatarios a través de múltiples medios de distribución. Los medios incluyen faxes, correos electrónicos, correo por vía marítima o terrestre, mensajería de SMS y archivo (y están adaptados a nuevos tipos que puedan desarrollarse en el futuro). Se usa una sola interfaz para recibir información para su distribución, incluidos uno o más documentos de plantilla y datos específicos de cada destinatario. Al menos un documento basado en la información recibida se transmite usando una entrega específica para cada destinatario según las preferencias de envío de los destinatarios. Puede producirse una transmisión escalonada del documento usando un medio de distribución diferente para cualquiera de los destinatarios en los que falla la transmisión realizada por los medios de distribución especificados. La etapa de escalonamiento puede depender de la información de estado de una portadora relacionada con la entrega del documento a cada destinatario. En el documento US5815555 se describe un procedimiento de entrega certificada de la transmisión de correo electrónico a través de una red telefónica. El procedimiento incluye las etapas de detectar una solicitud de certificación de correo electrónico desde un ordenador origen a un ordenador destino mediante un controlador de la red telefónica y de almacenar una copia de la transmisión de correo electrónico en el controlador. El procedimiento incluye además la etapa de certificar la entrega de la transmisión de correo electrónico haciendo corresponder una copia de la transmisión de correo electrónico recibida por el ordenador de destino con la copia almacenada. Finalmente, el documento US2004177048 da a conocer un procedimiento y un aparato para clasificar, priorizar, identificar, gestionar y controlar de otro modo (en términos generales, “controlar”) una comunicación. Puede usarse franqueo para asociar un valor y una clase a una comunicación. La comunicación puede asociarse al franqueo a través de un procedimiento para seleccionar un franqueo asociado a un valor de entre una pluralidad de tipos de franqueo, donde cada uno de los tipos de franqueo presenta un valor preasignado, que asocia el franqueo a la comunicación, y para iniciar la transmisión de la comunicación franqueada a través de una red. El valor puede incluir cualquier dato importante para las partes, incluido, por ejemplo, dinero, crédito (o intención de pago), millas de viajero frecuente, etc. “Franquear” una comunicación asocia generalmente alguna indicación de valor y/o una clase de servicio a una comunicación.

DESCRIPCIÓN DE LA INVENCIÓN

El objeto de invención de esta solicitud ofrece una solución con respecto a las desventajas previamente explicadas

mediante un procedimiento de certificación sencillo, como se describe en la reivindicación 1.

DESCRIPCIÓN DE LOS DIBUJOS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con una realización preferida de la misma, se acompaña como parte integrante de dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

Figura 1.- Muestra un diagrama de flujo de una realización preferida del método objeto de esta invención.

Figura 2.- Muestra un diagrama de flujo de una realización preferida de la creación de un certificado digital.

Figura 3.- Muestra un diagrama de flujo de una realización preferida del método en caso de que la copia del correo electrónico no pueda ser entregada al destinatario.

Figura 4.- Muestra un diagrama de flujo de una realización preferida del método de autenticación del usuario emisor.

REALIZACIÓN PREFERIDA DE LA INVENCIÓN

En la figura 1 se representa una realización preferida del método de certificación de correo electrónico objeto de la invención, que comprende el envío de un mensaje electrónico de un usuario emisor (1) a un destinatario (2).

El usuario emisor (1), que es cliente de la entidad certificadora, envía el mensaje electrónico que desea certificar a la dirección electrónica de destino, es decir, al destinatario (2) a través de una ruta inicial (3), que es la ruta convencional para el envío de mensajes electrónicos, y envía también una copia a la entidad certificadora, es decir, a través de una segunda ruta (10) distinta de la primera ruta (3) en la que un servidor de correos entrantes (11) recibe la referida copia. En la realización preferida mostrada, la unidad de procesamiento de datos (11) que gestiona el proceso de certificación coincide con el servidor de correos entrantes (11).

Por lo tanto, el usuario emisor (1) utiliza su proveedor de correo electrónico habitual, entregando el correo electrónico al destinatario o destinatarios (2). Para ello, un servidor de correo inicial (5) enviará una copia del correo electrónico a cada una de las direcciones destino especificadas por el usuario emisor (1) y un servidor de correo destino (6) recoge el correo electrónico para que finalmente el destinatario (2) pueda leerlo, no sufriendo este correo electrónico ninguna manipulación por parte de la entidad certificadora ni del sistema de certificación.

Adicionalmente, el método puede comprender la etapa de almacenar en una base de datos (12) una copia del correo electrónico o incluso la unidad de procesamiento (11) puede descomponer previamente la copia del correo electrónico en los diferentes objetos que lo conforman: origen, destino o destinos, ficheros adjuntos, clasificación de los ficheros adjuntos y finalmente la numeración de todos los objetos con su asignación al usuario emisor (1).

Como realización preferida de los ficheros adjuntos, estos pueden consistir en una factura, queriéndose en este caso certificar que la factura ha sido entregada al destinatario (2) de la misma.

Una vez descompuestas, indexadas y clasificadas todas sus partes, la copia del correo electrónico se envía insertando una indicación particular, que puede ser incluir en el correo electrónico el siguiente texto: CORREO ELECTRÓNICO CERTIFICADO o incluso más concretamente, FACTURA CERTIFICADA, si lo que se quiere certificar es el contenido de una factura incluida en los datos adjuntos. Posteriormente se realiza una nueva copia en una segunda base de datos (13) y se envía al servidor de correos salientes (14) del sistema de certificación. El servidor de correos salientes (14) lo entregará al servidor de destino (6), en donde quedará disponible para el destinatario (2).

Por lo tanto, el destinatario (2) recibe dos correos electrónicos. Uno es el correo electrónico original del usuario emisor (1), que utiliza sus propios servidores (5, 6), por lo tanto, a través de una ruta inicial (3), y el otro es un correo electrónico reenviado por el sistema de certificación de la entidad certificadora a través de una segunda ruta (10) con la indicación de certificación particular, por ejemplo, CORREO ELECTRÓNICO CERTIFICADO o FACTURA CERTIFICADA.

Si la copia del correo electrónico tenía una dirección de correo electrónico correcta y ha podido ser entregada al

servidor (6), el proceso de certificación continúa, cuya realización preferida se muestra en la figura 2. En el caso de que no haya podido ser entregada o bien la dirección no existiera, el proceso de certificación continúa según la realización preferida incluida en la figura 3.

Una vez entregada la copia del correo electrónico al servidor (6), el servidor de correos salientes (14) recibe los datos de notificación relativos a la entrega de la transmisión de la copia del correo electrónico y los envía a la unidad de procesamiento (11) que gestiona el proceso de certificación.

Una vez recibidas las indicaciones de envío, las etapas, las incidencias o cualquier información que pueda ser útil al proceso de certificación, la unidad de procesamiento (11) crea, en la realización preferida mostrada en la figura 2, un documento electrónico, por ejemplo en formato PDF, que incluye los datos del usuario emisor (1), la fecha de emisión, el contenido, los ficheros adjuntos si los hubiera y finalmente la fecha y hora de la entrega de la copia del correo electrónico.

Una vez creado el documento electrónico, se firma digitalmente mediante un algoritmo de firma digital para la creación de un certificado (4).

Adicionalmente se puede efectuar una suma digital de todo el contenido anterior, es decir, del documento electrónico y de la firma digital, y se envía a un cronofechador de confianza (20), con el fin de obtener un documento electrónico con dos firmas electrónicas de dos entidades para dar mayor refuerzo legal al propio certificado (4).

Una vez se tiene el fichero final o certificado (4), se envía al usuario emisor (1) descontando primeramente el coste de su cuenta de crédito y después se entrega al servidor de correos salientes (14). Este servidor (14) envía un correo electrónico, que incluye el certificado (4), al usuario emisor (1).

En la figura 3 se representa una realización preferida de un diagrama de flujo en el que la copia del mensaje electrónico no puede ser entregada al destinatario (2). Si el correo electrónico no puede ser entregado, bien porque el destinatario (2) no existe, bien porque el dominio no se encuentra operativo, se reintenta durante un periodo de, por ejemplo, 24 horas.

Si finalmente puede ser entregado, el proceso continúa según lo anteriormente explicado, pero si no puede ser entregado, el servidor de correos salientes (14) del sistema de certificación de la entidad certificadora recibe los datos de las transacciones realizadas, que se envían a la unidad de procesamiento (11).

Una vez recibidas las indicaciones de envío, las etapas, las incidencias y cualquier información que pueda ser útil al proceso de certificación, la unidad de procesamiento (11) crea, en la realización preferida mostrada en la figura 3, un documento electrónico, por ejemplo en formato PDF, que incluye los datos del usuario emisor (1), la fecha de emisión, el contenido, los ficheros adjuntos si los hubiera y finalmente fecha y hora del intento de entrega de la copia del correo electrónico.

Una vez creado este documento electrónico, se firma digitalmente mediante un algoritmo de firma digital, creando el certificado (4).

Adicionalmente se puede efectuar una suma digital de todo el contenido anterior, es decir, del documento electrónico y de la firma digital, y se envía a un cronofechador de confianza (20), con el fin de obtener un documento electrónico con dos firmas electrónicas de dos entidades para dar mayor refuerzo legal al propio certificado (4).

Una vez se tiene el fichero final o certificado (4), se envía al usuario emisor (1) descontando primeramente el coste de su cuenta de crédito y después se entrega al servidor de correos salientes (14). Este servidor (14) envía un correo electrónico, que incluye el certificado (4), al usuario emisor (1).

En la figura 4 se representa una realización preferida de la etapa previa en la que el usuario emisor (1) inicia la conexión con la unidad de procesamiento (11) de la entidad certificadora.

Este usuario emisor (1) puede entrar con diferentes sistemas de acceso, por ejemplo un ordenador personal, una tableta, un teléfono inteligente o cualquier dispositivo que le permita navegar a través de Internet.

En la realización preferida mostrada, los usuarios emisores (1) acceden a un sistema web de control de acceso. Este sistema dispone de acceso a una base de datos en donde se encuentran los ficheros de información de los usuarios

emisores (1) con capacidad de certificación y el número de certificaciones que tienen disponibles, así como de su capacidad de operativa.

El usuario emisor (1) introduce su nombre de usuario y su contraseña; si ésta no es correcta, se le redirige a una ayuda del sistema donde se le explica cómo darse de alta, y vuelve a entrar en el sistema de autenticación.

Si el usuario se autentica correctamente, puede acceder a un menú donde puede especificarse características acerca de cómo tiene que ser el certificado (4) a emitir y desde qué direcciones se permite el certificado de los correos electrónicos. Una vez definidos estos parámetros, el usuario emisor (1) puede solicitar un periodo de procesamiento de certificación y ajustar su horario. Dicho de otro modo, a partir de un determinado momento da autorización al sistema de certificación para que entren correos electrónicos e iniciar el proceso de certificación.

Finalmente, si cuando se inicia el proceso, el usuario emisor (1) está en el periodo de entrega del correo a certificar, iniciará los procesos. En caso contrario se devuelve el correo indicando que está fuera de periodo o que se trata de un usuario emisor (1) desconocido.

Como alternativa, el usuario puede solicitar un testigo o símbolo cifrado para efectuar las peticiones de certificación sin necesidad de abrir una ventana vía web.

REIVINDICACIONES

1.- Método para la certificación del envío de correo electrónico desde un usuario emisor (1) a un destinatario (2), comprendiendo el método llevar a cabo en un sistema de certificación de envío de correo electrónico implementado por una operadora de telecomunicaciones, donde el usuario emisor (1) es un cliente de dicho sistema de certificación de envío de correo electrónico, comprendiendo dicho sistema de certificación de envío de correo electrónico al menos una unidad de procesamiento de datos (11) que puede funcionar al menos como un servidor de correos entrantes (11) y un servidor de correos salientes (14) que están interconectados, las siguientes etapas:

- enviar un correo electrónico desde el usuario emisor (1) a al menos una dirección electrónica de destino del destinatario (2) a través de una ruta inicial (3) mediante un servidor de correo inicial (5) y un servidor de correo de destino (6),
- enviar, desde el usuario transmisor (1), una copia del correo electrónico enviado en la etapa anterior al sistema de certificación de envío de correo electrónico a través de una segunda ruta (10),
- recibir dicha copia del correo electrónico en el servidor de correos entrantes (11) del sistema de certificación,
- insertar una indicación particular en dicha copia del correo electrónico mediante la unidad de procesamiento (11), donde la indicación particular comprende la sentencia FACTURA CERTIFICADA,
- enviar a través del servidor de correos salientes (14) un segundo correo electrónico que comprende la copia del correo electrónico con la indicación particular,
- entregar al servidor de correo de destino (6) el segundo correo electrónico que comprende la copia del correo electrónico con la indicación particular,
- entregar al destinatario (2):

    - el correo electrónico a través de la ruta inicial (3),
    - la copia del correo electrónico a través de la segunda ruta (10),

    donde dicha copia del correo electrónico comprende la indicación particular,
- recibir en el servidor de correos entrantes (11) datos relativos a la entrega del segundo correo electrónico desde el servidor de correos salientes (14),
- generar, en la unidad de procesamiento (11), un documento electrónico que comprende datos relativos a las etapas anteriores,
- aplicar una firma digital al documento electrónico de la etapa anterior para la creación de un certificado electrónico (4),
- enviar desde el servidor de correos salientes (14) el documento electrónico a una tercera parte para llevar a cabo una segunda firma digital, y
- entregar el certificado electrónico (4) al usuario emisor (1) desde la unidad de procesamiento (11).

2.- Método para la certificación del envío de correo electrónico, de acuerdo con la reivindicación 1, caracterizado porque comprende además la etapa de almacenar, en una base de datos (12), la copia del correo electrónico.

3.- Método para la certificación del envío de correo electrónico, de acuerdo con la reivindicación 2, caracterizado porque antes de almacenarla en la base de datos (12), la unidad de procesamiento (11) realiza una descomposición de la copia del primer correo electrónico en al menos: origen, destino, adjuntos.

4.- Método para la certificación del envío de correo electrónico, de acuerdo con la reivindicación 3, caracterizado porque, adicionalmente, la unidad de procesamiento (11) numera todos los elementos en los que se descompone la copia del primer correo electrónico y los asigna al usuario emisor (1).

5.- Método para la certificación del envío de correo electrónico, de acuerdo con una cualquiera de las reivindicaciones anteriores, caracterizado porque la unidad de procesamiento (11) descuenta una cantidad de la cuenta del usuario emisor (1).

6.- Método para la certificación del envío de correo electrónico, de acuerdo con una cualquiera de las reivindicaciones anteriores, caracterizado porque comprende la etapa inicial de autenticar el usuario emisor (1) en el sistema de certificación.

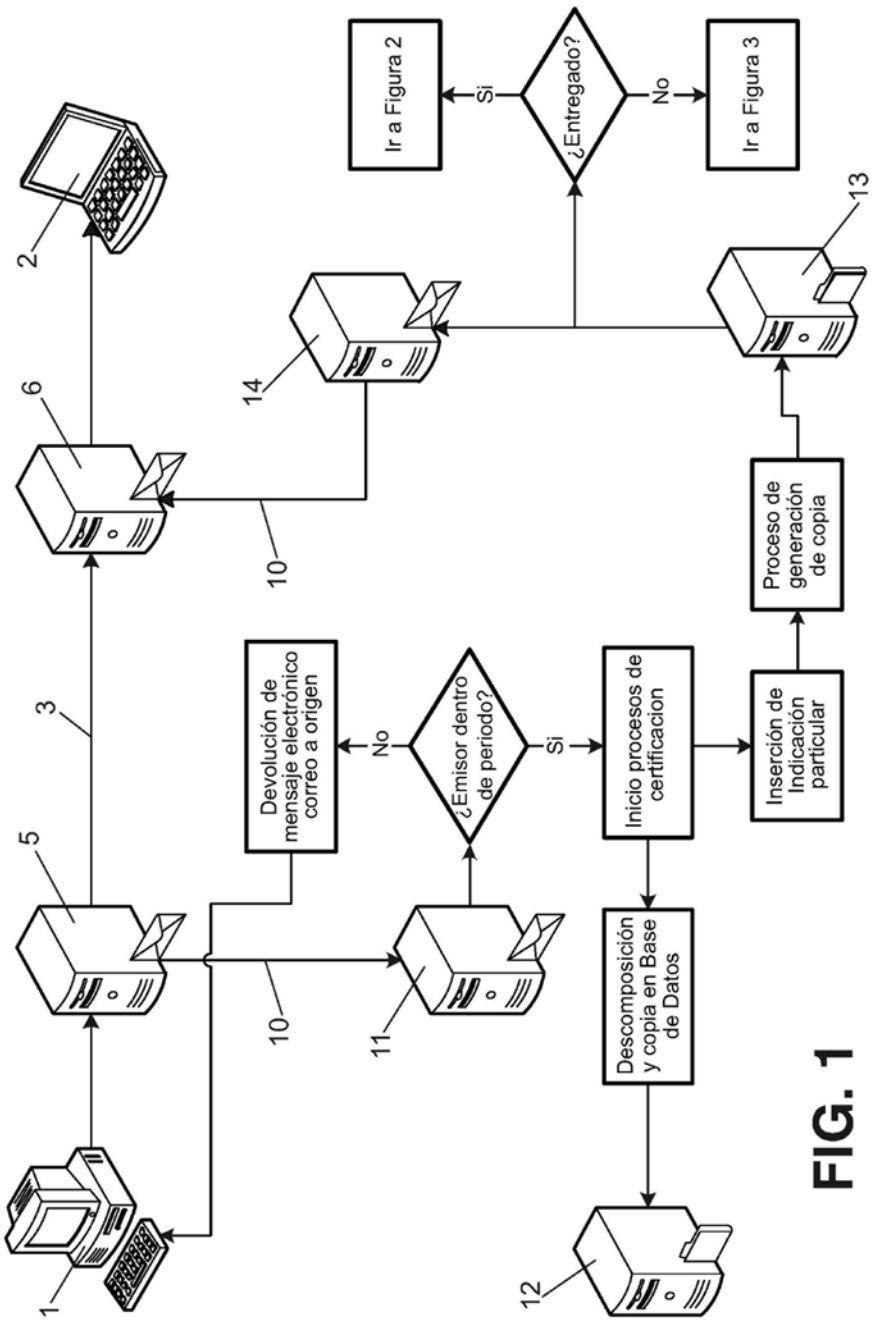
Ir a Figura 2
Si
¿Entregado?
No
Ir a Figura 3
2
13
14
6
10
Proceso de generación de copia
Devolución de mensaje electrónico correo a origen
No
¿Emisor dentro de periodo?
Si
Inicio procesos de certificacion
Inserción de Indicación particular
3
5
Descomposición y copia en Base de Datos
10
11
12
1

FIG. 1

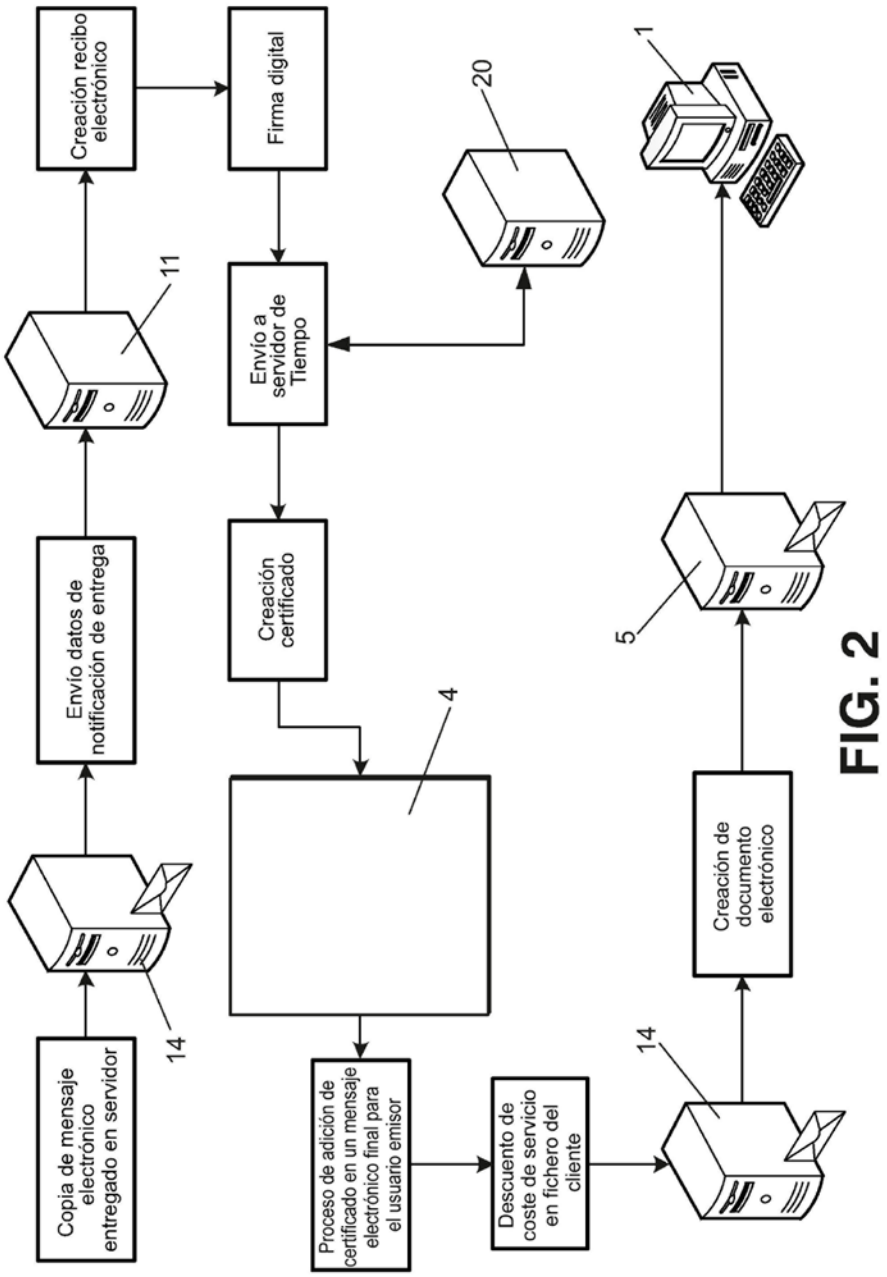
Creación recibo electrónico
Firma digital
20
1
11
Envío a servidor de Tiempo
Envío datos de notificación de entrega
Creación certificado
4
5
14
Copia de mensaje electrónico entregado en servidor
Proceso de adición de certificado en un mensaje electrónico final para el usuario emisor
Descuento de coste de servicio en fichero del cliente
14
Creación de documento electrónico

FIG. 2

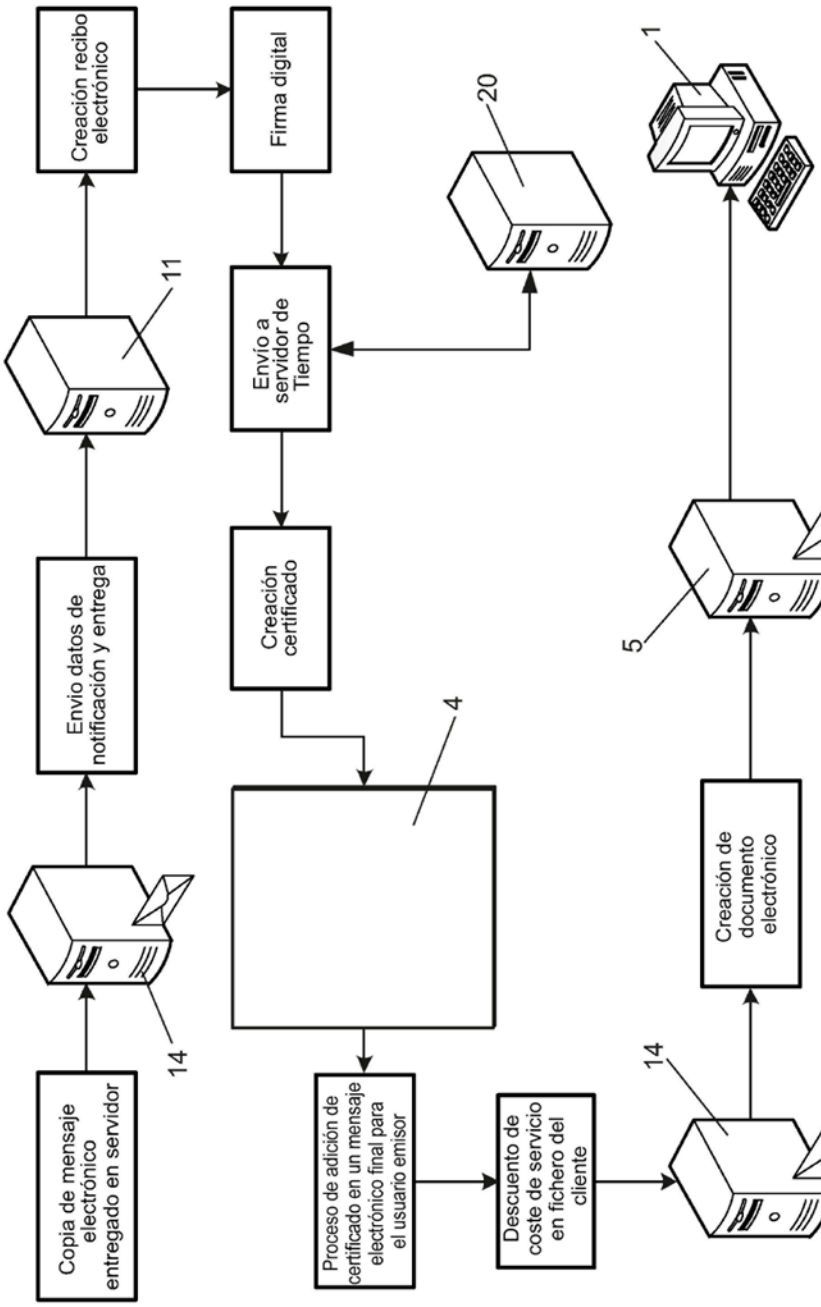
Copia de mensaje electrónico entregado en servidor
Envio datos de notificación y entrega
Creación recibo electrónico
Proceso de adición de certificado en un mensaje electrónico final para el usuario emisor
Descuento de coste de servicio en fichero del cliente
Creación de documento electrónico
Creación certificado
Envío a servidor de Tiempo
Firma digital
14
11
4
20
1
5
14

FIG. 3

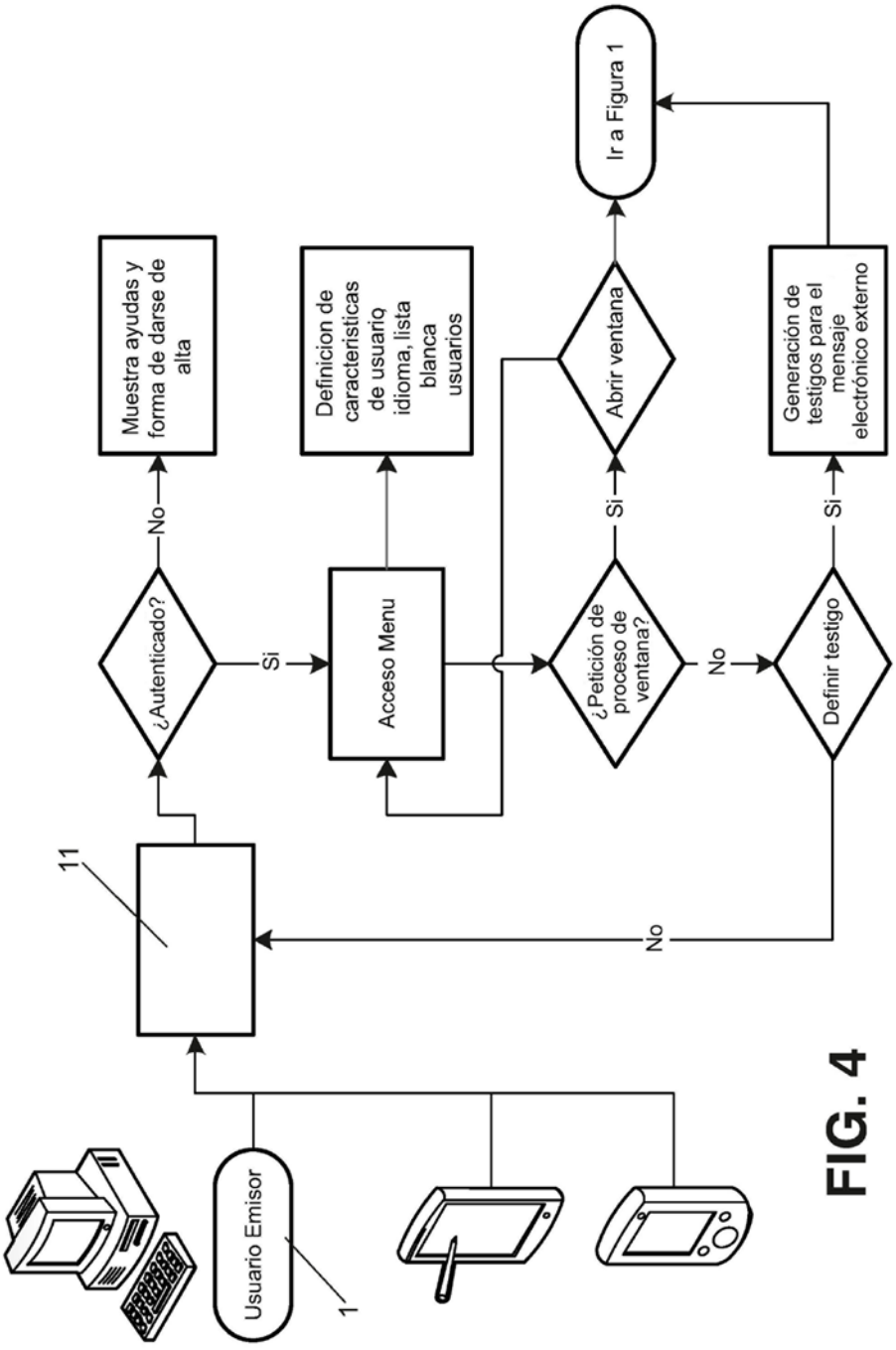
Usuario Emisor
1
11
¿Autenticado?
No
Si
Muestra ayudas y forma de darse de alta
Acceso Menu
Definicion de caracteristicas de usuario idioma, lista blanca usuarios
¿Petición de proceso de ventana?
Si
No
Abrir ventana
Ir a Figura 1
Definir testigo
Si
No
Generación de testigos para el mensaje electrónico externo

FIG. 4