(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 765 706**

(51) Int. CI.:

G06Q 10/10 (2012.01)
H04L 29/06 (2006.01)
H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.12.2015 E 15382665 (6)**

(97) Fecha y número de publicación de la concesión europea: **13.11.2019 EP 3188435**

(54) Título: **Método para certificar un correo electrónico que comprende una firma digital fiable por un operador de telecomunicaciones**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.06.2020

(73) Titular/es:

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

(72) Inventor/es:

SAPENA SOLER, FRANCISCO

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método para certificar un correo electrónico que comprende una firma digital fiable por un operador de telecomunicaciones

Objeto de la invención

El objeto de la invención es un método para que un operador de telecomunicaciones sea capaz de recibir, redireccionar, entregar y certificar correos electrónicos firmados con una firma electrónica reconocida de cualquier cliente de usuario transmisor del operador a uno o varios receptores no clientes del operador de forma no intrusiva, respetando las firmas electrónicas de los correos originales para evitar romper la cadena de custodia, reenviar el mismo intacto con las firmas originales y adaptado a la norma DMARC, generar prueba de todas las operaciones de transacciones para, finalmente, firmar el mismo digitalmente como el operador de telecomunicaciones y entregar a clientes de usuarios transmisores un certificado como una tercera parte confiable con los detalles del transmisor, fecha de transmisión, el texto completo enviado, el correo original firmado electrónicamente por el usuario que respeta la firma original, fecha y hora de entrega y las circunstancias finales en el caso de no entrega o retardo en la entrega al receptor no cliente.

Antecedentes de la invención

Se sabe que en la actualidad las comunicaciones electrónicas se han vuelto una herramienta esencial e indispensable para cualquier operación, tanto legal como ilegal. Comunicaciones se usan para todos tipos de movimientos, generación de llamadas, mensajes, etcétera, desde un origen a un destino.

Operadores de telecomunicaciones son las partes que proporcionan las infraestructuras que gestionan, dirigen y almacenan una gran parte de este tráfico. Estos operadores de telecomunicaciones están sometidos a regulación, entre otras, para el uso del espectro de radio que está limitado, o para el uso de recursos de numeración telefónica que también son finitos.

Operadores de telecomunicaciones además registran las operaciones hechas por usuarios con el objetivo, entre otros, de cobrar, registrar números asociados a los mismos, como referencias de facturación, y para registrar cualquier otro detalle transaccional usado para facturar al usuario. Estos registros se conservan para posteriores verificaciones de cobros y/o supervisión de tráfico en la parte del usuario.

Ocasionalmente, las autoridades judiciales solicitan a operadores de telecomunicaciones que proporcionen detalles registrados de transacciones electrónicas hechas, ya que consideran a los mismos terceras partes confiables para el propósito de proporcionar estos detalles, junto con cualquier otro detalle que podría ayudar a determinar los individuos privados o entidades legales que han efectuado la acción de interés.

Una vez que se han localizado los detalles solicitados por las autoridades judiciales, el operador emite un certificado que declara explícitamente los detalles transaccionales solicitados, frecuencia, destinos y cualquier otra información solicitada por la autoridad judicial pertinente.

Esta metodología, cuando se solicita por cualquiera de las partes a un operador de telecomunicaciones y presenta como prueba, ha sido recientemente aceptada como prueba por nuestra corte suprema (ATS 2501/2013, Corte Suprema de España, Cámara Civil).

El estado de la técnica es familiar con varios métodos y sistemas para el envío de correo electrónico certificado, basándose algunos en el envío en la parte del cliente de un enlace a un entorno web controlado por una tercera parte confiable en la que se descarga el contenido certificado, teniendo el inconveniente básico de requerir la voluntad de la parte notificada de descargar dicho contenido para generar el certificado, y otros en los que se añaden verificaciones digitales al contenido y que simulan ser el transmisor, reenviando el mismo al destino. Este último tiene tres inconvenientes serios:

a) En el reenvío en nombre del usuario, la firma electrónica reconocida se rompe cuando las condiciones de origen cambian totalmente, rompiendo la cadena de custodia y generando desconfianza.
b) Añadir verificaciones dentro para comprobación posterior de la certificación del correo electrónico de nuevo rompe la firma electrónica originalmente reconocida y la cadena de custodia nuevamente.
c) En el reenvío en nombre del usuario como si fuera el usuario, el correo electrónico certificado choca con la norma DMARC que se está imponiendo como la norma a una escala mundial, evitando la entrega efectiva del correo electrónico certificado.

La invención que es el objeto de esta solicitud proporciona una solución a las desventajas mencionadas anteriormente, sin requerir una descarga posterior del contenido a certificar, respetando tanto la firma electrónica reconocida original del usuario para mantener la cadena de custodia, y la total funcionalidad del servicio bajo la norma DMARC; resultando el proceso en un certificado emitido por un operador de telecomunicaciones que contiene el mensaje original sin

romper las firmas reconocidas originales que acredita que el operador envió ese contenido de correo electrónico a un destino, en una fecha y hora determinadas y que se entregó finalmente o no a su representante electrónico oficial, incluyendo también los detalles de transmisión, detalles transmitidos, adjuntos, un único número de registro y cualquier detalle transaccional usado.

El documento RFC 6109 "La Posta Elettronica Certificata - Italian Certified Electronic Mail" divulga un método para certificar la entrega de correo electrónico.

Descripción de la invención

De acuerdo con lo mencionado anteriormente, el objeto de la invención es un método para el envío de un correo electrónico con una firma electrónica reconocida a certificar por un operador de comunicaciones de tal forma que el destino recibe dos copias, la original desde el cliente y la copia desde el operador de telecomunicaciones sin simular ser el cliente original, respetando las firmas electrónicas reconocidas y la cadena de custodia. El cliente del operador o transmisor, recibe un certificado de acuerdo con quién envió el correo electrónico original, incluyendo el correo original, el contenido visible, fecha, hora y trazabilidad del mismo, un único número de transacción; y finalmente la fecha, hora y circunstancias de la entrega si tal cosa fuera posible.

El método para crear el correo electrónico certificado por un operador de telecomunicaciones que es el objeto de la invención se caracteriza por que comprende las siguientes etapas y por que incorpora al menos un servidor de correo externo del cliente del operador, un servidor de destino del correo certificado, un servidor de correo entrante del operador, un servidor de base de datos de copias y elementos fragmentados, un servidor de correo de salida del operador, un servidor de indicación de tiempo TSA, un servidor de base de datos de elementos enviados y una unidad de procesamiento de datos como el servidor de certificación todos interconectados entre sí.

- Transmisión por el cliente del operador de telecomunicaciones de un correo electrónico a un destino determinado usando cualquier plataforma a través de su proveedor de internet, copiando una dirección de correo del servidor del operador de telecomunicaciones, por ejemplo, correo@certificado.lleida.net
- Recepción del correo electrónico clásico en el destino por medio de su representante digital autorizado.
- Recepción de la copia en el servidor de correo entrante del operador del mensaje transmitido por el cliente de usuario del operador de telecomunicaciones.
- Comprobar que el usuario está autorizado, tiene crédito para certificar correos y continuar a inserción y registro en la base de datos del texto y componentes recibidos.
- Creación en la unidad de procesamiento de datos del operador de telecomunicaciones de un correo electrónico que se transmitirá desde una dirección del servidor del operador de telecomunicaciones noreply@mailcert.lleida.net encapsulando el contenido enviado por el cliente del operador para respetar las firmas digitales originales reconocidas, insertando específicamente en el asunto del correo electrónico CORREO ELECTRÓNICO CERTIFICADO.
- Envío del correo encapsulado en la parte del servidor de correo electrónico saliente.
- Aceptación o no por el representante digital autorizado del destino no de cliente del correo electrónico encapsulado,
- Generación final del certificado del operador de telecomunicaciones, incluyendo el correo original que respeta las firmas digitales reconocidas, los detalles enviados, recibidos, fechas y horas de transmisión y recepción y aplicación de la firma digital reconocida y la indicación de tiempo en la parte del operador de telecomunicaciones.
- Enviar del certificado al usuario transmisor a través del servidor de correo.

De acuerdo con lo anterior, el método que es el objeto de la invención ofrece asimismo la ventaja de no manipular el correo original, manteniendo la cadena de custodia y permitiendo el uso de formas digitales reconocidas por el usuario, siendo asimismo compatible con la norma DMARC, ya que la copia encapsulada del correo no se reenvía en nombre del usuario, sino en nombre del operador de telecomunicaciones. Finalmente, se genera evidencia de transmisión, recepción y aceptación del contenido en la parte de un operador de telecomunicaciones. La invención se define por las reivindicaciones adjuntas.

Descripción de los dibujos

Para complementar la descripción hecha y para el propósito de contribuir a un mejor entendimiento de la invención, de acuerdo con un ejemplo preferido de una realización práctica de la misma, se adjunta un conjunto de dibujos como una parte integral de dicha descripción, en el que por medio de ilustración y no limitación, los siguientes se han representado:

La Figura 1.- muestra un diagrama de flujo de un ejemplo de realización del método que es el objeto de la invención del inicio de creación del correo electrónico certificado y la entrega o no de la copia encapsulada.
La Figura 2.- muestra un diagrama de flujo de un ejemplo de realización del método que es el objeto de la invención de la composición y envío del certificado final en los casos de entrega o no entrega del correo electrónico encapsulado.

Realización preferida de la invención

A la luz de las Figuras 1 y 2 en el que se representan una serie de diagramas haciendo referencia a un método que es el objeto de la invención, método previsto para certificar correos electrónicos que contienen una firma electrónica reconocida en la parte de un operador de telecomunicaciones que comprende desde enviar un correo electrónico desde un transmisor (1,2,3), usuario del operador de telecomunicaciones, a través de recepción del certificado que confirma que el envío se efectuó, se entregó, con el contenido y detalles de transmisión usados, todo lo anterior firmado con una firma electrónica reconocida del operador e indicación de tiempo de una tercera parte.

El cliente de usuario transmisor del operador de telecomunicaciones, cuando desea enviar un correo electrónico certificado envía el correo a través de cualquier plataforma, PC, Tableta o teléfono móvil copiando una dirección de correo de un servidor de correo entrante del operador de telecomunicaciones tal como, por ejemplo, correo@certificado.lleida.net. Para hacer esto, en la parte del transmisor (1,2,3), que es un usuario del operador de telecomunicaciones, al menos se genera un correo electrónico, para hacer que el correo electrónico llegue a un servidor de correo cliente del operador de telecomunicaciones (4,15), por ejemplo, el correo electrónico se envía al servidor de correo cliente de Lleida.net, perteneciendo este último a cualquier proveedor de internet, y se entrega a un servidor de destino que por propósitos legales es el representante electrónico autorizado, en otras palabras se hace llegar a un servidor de destino de correo (7, 24) a través de la internet (5) para hacer que llegue a un destino de correo certificado (8,25), ya que es a nivel de internet en el que los mensajes pueden entregarse a un destino determinado, asimismo una copia de este mensaje se entrega a un servidor de correo entrante del operador (9), el servidor de correo entrante de Lleida.net en este ejemplo.

El servidor de correo entrante del operador (9) envía el correo electrónico a un servidor de procesamiento de datos de certificación (Mailcert) que forma parte del operador de telecomunicaciones y comprobará si el usuario está en la lista blanca, en otras palabras, está registrado en el sistema para ser capaz de enviar correos electrónicos certificados. Si no está registrado, el correo se ignora, si está registrado continúa a verificar que el usuario tiene crédito, esto implica comprobar (10) que el usuario (1,2,3) tiene privilegios de certificación por medio de comparación con una lista de usuarios/privilegios, comprobar que se efectúa por medio de enviar el correo electrónico a un servidor de procesamiento de datos de certificación.

Si el usuario en cuestión no tiene ningún crédito, se genera un correo electrónico que indica la ausencia del mismo, enviando el mismo a un servidor de correo de salida del operador (23,26,38,50) que entregará el mismo finalmente al usuario (1,2,3) que es el cliente de usuario del operador de comunicaciones.

Si el usuario no tiene crédito a continuación procede a certificar (17) el correo electrónico en el que dicha certificación a su vez comprende generar una copia (18) del correo electrónico y descomponer el correo electrónico en sus partes, en el que dichas partes comprenden: detalles de transmisión, detalles de recepción y contenido del correo para el procesamiento del mismo, siendo dichos detalles guardados preferentemente en una primera base de datos (19,32,43) junto con la copia (18).

Posteriormente la copia (18) del correo electrónico se encapsula (20) en un contenedor y se genera un correo certificado (21) que comprende la copia encapsulada (18) del correo electrónico a continuación se hace llegar a un servidor de correo de salida del operador (23,26), para hacer que el correo certificado (21) llegue al servidor de destino de correo (7, 24) desde el servidor de correo de salida del operador (23,26,38,50) y para hacer que el correo certificado (21) llegue desde el servidor de destino de correo (7, 24) a: el destino de correo certificado (8,25), y al servidor de correo de salida del operador (23,26,38,50).

Se genera un correo certificado (21) desde una dirección de correo electrónico con origen en el servidor de procesamiento de datos de certificación que forma parte del operador de telecomunicaciones como puede ser: service@correo electrónicocert.lleida.net siendo el asunto del mensaje CORREO ELECTRÓNICO CERTIFICADO, añadiendo el texto del asunto original, y tantos textos de control como puedan considerarse necesarios. El hecho de enviarse como servidor de certificación service@correo electrónicocert.lleida.net desde el operador de telecomunicaciones y no poniendo como origen la dirección de correo electrónico original del cliente permite que el servicio cumpla con DMARC ya que no suplanta al cliente, a pesar de proporcionarnos autorización para entregar un correo electrónico en nombre del cliente.

Dentro del texto del correo certificado (21) se incluye un anuncio e indicaciones que confirman que es un mensaje certificado y finalmente se encapsula (20) el mismo, en otras palabras, todo el mensaje original se incluye para el propósito de respetar las firmas electrónicas reconocidas originales para evitar cualquier manipulación del interior rompiendo la firma reconocida y generar desconfianza de la veracidad del mensaje. La copia encapsulada (18) del correo electrónico se guarda en una segunda base de datos (22,33,46) y se hace llegar al servidor de correo de salida del operador (23,26,38,50) para el envío del mismo.

El servidor de correo de salida del operador (23, 26, 38, 50) entregará la copia encapsulada (18) del correo electrónico, para su entrega, pero aún así esperará durante un tiempo posterior de entre 10 minutos y una hora para una respuesta de rechazo posterior, en otras palabras, inicialmente el servidor de correo electrónico en el destino aceptará todo en primera instancia y posteriormente rechazará el mismo, siendo esto un comportamiento al que el sistema se autoajusta

automáticamente.

Si el correo electrónico certificado se pudo entregar finalmente, el método continúa al proceso OK de la Figura 2 y si el correo electrónico certificado podría no entregarse a continuación continúa al proceso NOOK también presente en la Figura 2.

El servidor de correo de salida del operador (23, 26, 38, 50), entregará el correo electrónico encapsulado a su representante digital autorizado, para su entrega, pero incluso así esperará durante un tiempo posterior de entre 10 minutos y una hora para una respuesta de rechazo posterior, en otras palabras, inicialmente un servidor de destino de correo (7, 24) acepta todo en primera instancia y posteriormente rechaza el mismo, siendo esto un comportamiento al que el método descrito en este documento se autoajusta automáticamente.

Existe una comprobación de entrega (27) del correo certificado (21) en el destino de correo certificado (8,25). Si el correo certificado (21) se pudo entregar finalmente, el método continúa al proceso OK de la Figura 2 y si el correo electrónico certificado no se pudo entregar el método continúa al proceso NOOK también presente en la Figura 2.

Con el correo certificado (21) entregado, el método continúa al proceso de generar un certificado (37,49) del operador en sí mismo, en otras palabras el correo certificado (21) se hace llegar desde el servidor de destino de correo (7, 24) al destino de correo certificado (8,25), y al servidor de correo de salida del operador (23,26,38,50) dado que en efectuar la comprobación de entrega (27) del correo certificado (21) en el destino de correo certificado (8,25) se obtuvo un OK. A continuación, se genera un certificado (37,49) por medio de un servidor de certificación (30,41) del operador de telecomunicaciones en el que dicho certificado (37,49) comprende una primera parte (31,42) que a su vez comprende detalles de transmisión, detalles de recepción y contenido del correo, y una segunda parte (34,45) que a su vez comprende detalles de la llegada del certificado (21) al servidor de correo de salida del operador (23,26), y una firma digital y una indicación de tiempo (35,48) del operador de telecomunicaciones.

Para hacer esto, el contenido y correos electrónicos originales se recuperan de la primera base de datos (19,32,43) de copia inicial que compone la primera parte del certificado (37, 49). Una vez que se hace esto, se verifica si el servidor de destino de correo (7, 24) está en la lista de rebote/listas negras, por medio de una verificación (44) posterior a la generación de la primera parte (31,42) en el que dicha verificación (44) comprende comprobar si el servidor de destino del correo electrónico certificado (8,25) está en una lista de servidores de rebote/listas negras que por defecto aceptan todos los mensajes y posteriormente rechazan los mismos cuando el destinatario del correspondiente correo certificado (8,25) no existe. En otras palabras, se verifica (44) si está o no en la lista de servidores que por defecto aceptan todos los mensajes y posteriormente rechazan los mismos cuando el usuario no existe, comprobando si ha llegado un mensaje de rechazo posterior desde el servidor de destino de correo (7, 24). Si ha llegado un mensaje de rechazo posterior a continuación el método continúa al proceso NOOK.

Si la verificación (44) da como resultado que el servidor de destino de correo certificado (8,25) está en la lista de servidores de rebote/listas negras, se procede a añadir al certificado (37,49) detalles que hacen referencia a la no existencia del destinatario en el servidor de destino de correo certificado (8,25). Si la verificación (44) da como resultado que el servidor de destino de correo (7, 24) no está en la lista negra o lista de rebote, la segunda parte del certificado se compone con todos los detalles transaccionales, añadiendo la indicación de tiempo (35,48) de una tercera parte y firmando el certificado (37,49) con la firma electrónica reconocida del operador de telecomunicaciones como se ha indicado previamente en la descripción del contenido de la segunda parte (34,45) del certificado (37,49).

Habiendo finalizado el certificado (37,49), se genera un correo electrónico al que se adjunta este certificado generado (37, 49), que se envía al servidor de correo de salida del operador de telecomunicaciones (23,26), que entregará el mismo finalmente al representante electrónico autorizado para entregar el mismo al cliente.

El proceso NOOK es el proceso que se usa cuando por cualquier circunstancia no ha sido posible entregar el correo certificado (21) al destino de correo certificado (8,25), enfatizando que en el proceso de enviar notificaciones fiables, tanto entrega como no entrega son igualmente importantes, dado que el objetivo es demostrar una voluntad expresa y explícita públicamente de enviar un contenido incluso si pudieran existir circunstancias que evitan la misma, transformando la notificación fiable en una diligente; en otras palabras, se ha hecho todo lo técnicamente posible para efectuar la entrega.

Una vez que se determina que el correo certificado (21) continua al proceso NOOK, el certificado (37,49) se recompone de nuevo identificando al destinatario e incluyendo los detalles de este último en el certificado (37,49) junto con todas las vicisitudes que han evitado la entrega efectiva del mensaje a su representante electrónico autorizado, por ejemplo, es posible añadir al certificado (37,49) detalles que hacen referencia a la no entrega tal como la hora de entrega intentada, dirección de entrega, identificación del destinatario, etc. Una vez que se completa el certificado (37,49), se firma electrónicamente con la firma digital reconocida del operador de telecomunicaciones y la indicación de tiempo de una tercera parte se añade al mismo.

Una vez que se firma el documento, se genera un correo electrónico al que se adjunta este documento en pdf y se envía por correo electrónico al transmisor (1,2,3), que es un usuario del operador de telecomunicaciones.

Con los certificados finalmente generados (37,49), el transmisor (1,2,3), que es un usuario del operador de telecomunicaciones, puede demonstrar de forma fiable que envió un correo certificado (21) a un destino de correo certificado determinado (8,25), usando su propia firma electrónica reconocida sin modificar el correo electrónico en ninguna de sus transacciones o evitando su entrega debido a las nuevas normas implementada en la internet.

REIVINDICACIONES

1. Método de certificación de correo electrónico firmado digitalmente, que se efectúa por medio de un operador de telecomunicaciones, comprendiendo el método:

i. generación por un transmisor (1,2,3), que es un usuario del operador de telecomunicaciones, de al menos un correo electrónico,
ii. hacer que el correo electrónico llegue a un servidor de correo cliente del operador de telecomunicaciones (4,15),
iii. enviar el correo electrónico a:

- un servidor de destino de correo (7, 24) a través de la internet (5) para hacer que llegue a un destino de correo certificado (8,25), y
- un servidor de correo entrante del operador de telecomunicaciones (9), y enviar el correo electrónico desde el servidor de correo entrante del operador de telecomunicaciones (9) a un servidor de procesamiento de datos de certificación que forma una parte del operador de telecomunicaciones,

iv. certificar (17), por el servidor de procesamiento de datos de certificación, el correo electrónico en el que dicha certificación a su vez comprende generar una copia (18) del correo electrónico y descomponer el correo electrónico en sus partes en el que dichas partes comprenden detalles de transmisión, detalles de recepción y contenido del correo,
el método de certificación de correo electrónico firmado digitalmente comprende además:
v. encapsular (20), por el servidor de procesamiento de datos de certificación, la copia (18) del correo electrónico en un contenedor,
vi. generar un correo certificado (21), por el servidor de procesamiento de datos de certificación, que comprende la copia encapsulada (18) del correo electrónico y hacer que llegue al servidor de correo de salida de un operador de telecomunicaciones (23, 26) desde el servidor de procesamiento de datos de certificación,
vii. hacer que el correo certificado (21) llegue al servidor de destino de correo (7, 24) desde el servidor de correo de salida del operador de telecomunicaciones (23,26,38,50),
viii. hacer que el correo certificado (21) llegue desde el servidor de destino de correo (7, 24) a:

- el destino de correo certificado (8,25), y
- el servidor de correo de salida del operador de telecomunicaciones (23,26,38,50),

ix. entregando el servidor de correo de salida del operador de telecomunicaciones (23,26,38,50) la copia encapsulada (18) del correo electrónico, para su entrega, esperando un tiempo posterior de entre 10 minutos y una hora para una respuesta de rechazo posterior para evitar que el servidor de destino de correo acepte todo en primera instancia y posteriormente rechace,
x. efectuar una comprobación de entrega (27) del correo certificado (21) en el destino de correo certificado (8,25),
xi. si el correo certificado se pudo entregar, generar un certificado (37,49) por medio de un servidor de certificación (30,41) del operador de telecomunicaciones en el que dicho certificado comprende:

a. una primera parte (31,42) que a su vez comprende: detalles de transmisión, detalles de recepción y contenido del correo, y
b. una segunda parte (34,45) que a su vez comprende detalles de la llegada del certificado (21) en el servidor de correo de salida del operador de telecomunicaciones (23,26),
en el que se efectúa una verificación (44) posterior a la generación de la primera parte (31,42), comprendiendo dicha verificación (44) comprobar si el servidor de destino de correo del correo electrónico certificado (8,25) está en una lista de servidores de rebote/listas negras que por defecto aceptan todos los mensajes y posteriormente rechazan los mismos cuando el destinatario del correspondiente correo certificado (8,25) no existe; de tal forma que el método comprende adicionalmente:

• añadir al certificado (37,49) detalles que hacen referencia a la no existencia del destinatario en el servidor de destino de correo certificado (8,25), cuando la verificación (44) da como resultado que el servidor de destino de correo certificado (8,25) está en la lista de servidores de rebote/listas negras, o
• componer la segunda parte (34,45) del certificado (37,49) con todos los detalles transaccionales, añadir una indicación de tiempo (35,48) de una tercera parte y firmar el certificado (37,49) con la firma electrónica del operador de telecomunicaciones, cuando el servidor de destino de correo (7, 24) no está en la lista negra o lista de rebote, y

xii. hacer que el certificado (37,49) llegue al transmisor (1,2,3).

2. Método de acuerdo con la reivindicación 1 comprendiendo además comprobar (10) que el transmisor (1,2,3) tiene privilegios de certificación por medio de comparación con una lista de usuarios/privilegios, comprobar que se efectúa por medio de enviar el correo electrónico a un servidor de procesamiento de datos de certificación.

3. Método de acuerdo con la reivindicación 1 comprendiendo además efectuar un vaciado de la copia (18) del correo

electrónico y sus partes, una vez que la copia (18) se ha descompuesto, en una primera base de datos (19,32,43).

4. Método de acuerdo con la reivindicación 1 comprendiendo además efectuar un vaciado del correo certificado (21) en una segunda base de datos 22,33,46) que comprende elementos que se han hecho llegar al servidor de correo de salida del operador de telecomunicaciones (23,26,38,50).

5. Método de acuerdo con cualquiera de las reivindicaciones anteriores en el que la comprobación de entrega (27) de etapa x da como resultado una no entrega del correo certificado (21) en el destino de correo certificado (8,25), comprendiendo el método además comprende añadir al certificado (37,49) detalles que hacen referencia a la no entrega en el que dichos detalles comprenden: hora de entrega intentada y dirección de entrega.

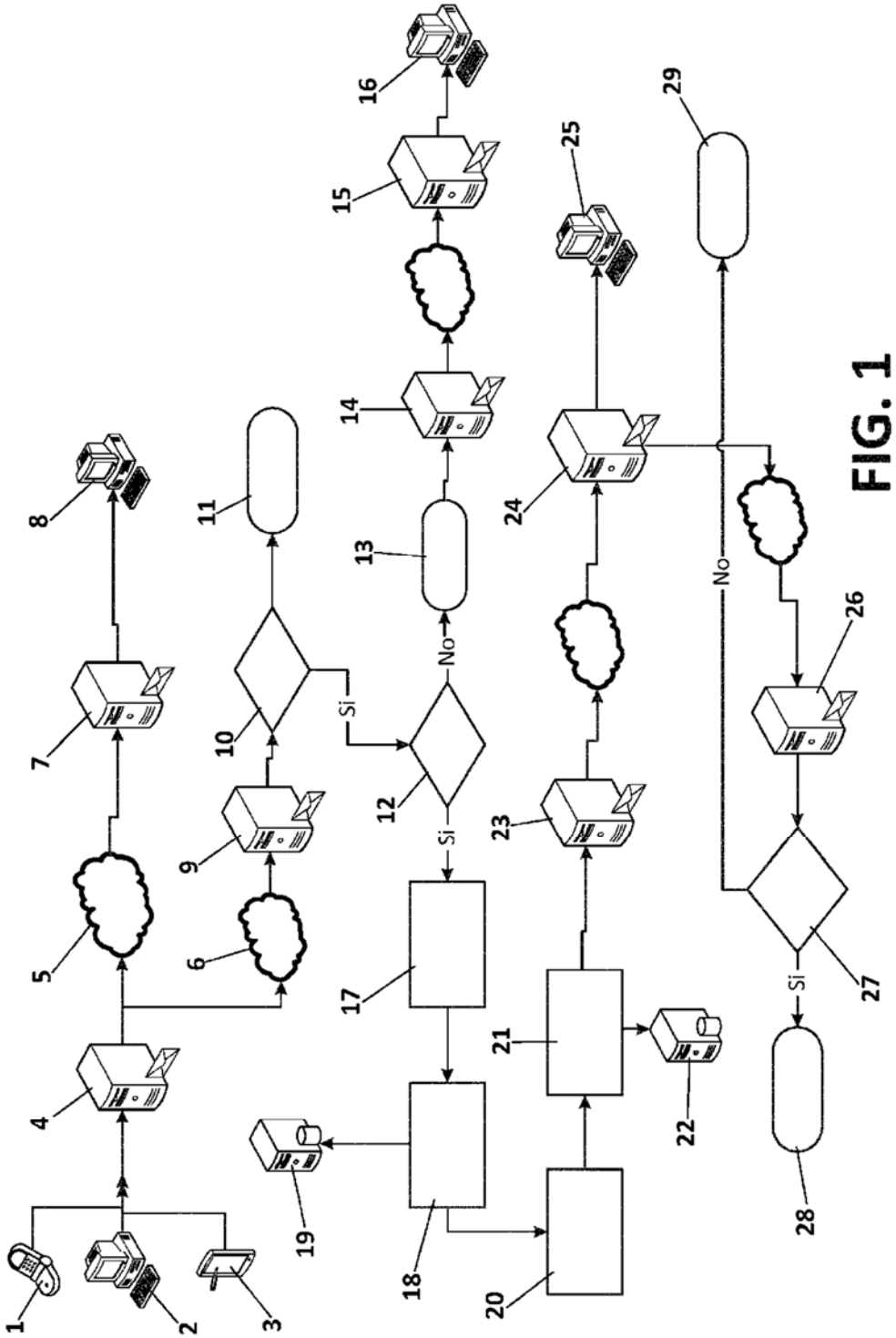
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
Si
No
Si
No
Si

FIG. 1

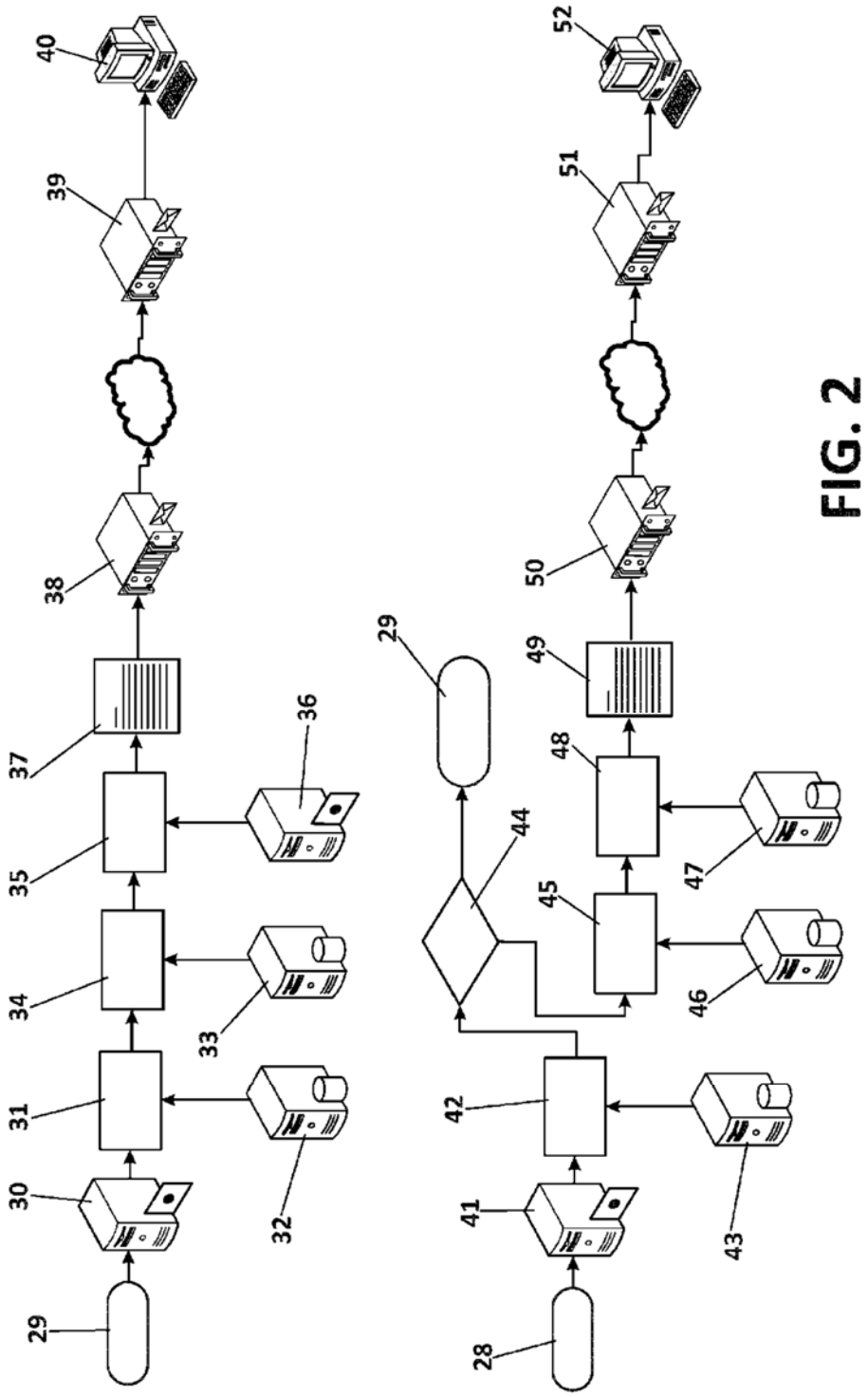
40
39
38
37
36
35
34
33
31
30
32
29
52
51
50
49
48
47
45
46
44
42
41
43
28
29

FIG. 2