(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 307 924**

(51) Int. Cl.:
H04L 12/58 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03721293 .3**
(96) Fecha de presentación : **21.02.2003**
(97) Número de publicación de la solicitud: **1476995**
(97) Fecha de publicación de la solicitud: **17.11.2004**

(54) Título: **Sistema y método para verificar la transmisión y la integridad de mensajes electrónicos.**

(30) Prioridad: **22.02.2002 US 991201**

(45) Fecha de publicación de la mención BOPI:
01.12.2008

(45) Fecha de la publicación del folleto de la patente:
01.12.2008

(73) Titular/es: **Rpost International Limited**
c/o Deloitte & Touche, Third Floor
Corner House, 20 Parliament Street
Hamilton, BM

(72) Inventor/es: **Tomkow, Terrence, A.**

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Sistema y método para verificar la transmisión y la integridad de mensajes electrónicos.

Antecedentes de personificaciones preferidas de la invención

I. Campo de la invención

Esta invención se refiere en general a un sistema y método para verificar la entrega y contenido de un mensaje electrónico y, más particularmente, a un sistema y método de proporcionar posteriormente una prueba con respecto a la entrega y el contenido de un mensaje de correo electrónico. Más específicamente, la invención se refiere a un sistema y método para enviar correo registrado a través de Internet y verificar a la vez la entrega y el contenido de un mensaje electrónico y proporcionar ulteriormente una prueba con respecto a la entrega y el contenido del mensaje de correo electrónico registrado.

II. Descripción de la técnica relacionada

En años recientes, el correo electrónico se ha vuelto una herramienta mercantil indispensable. El correo electrónico ha reemplazado al "correo caracol" para muchas prácticas mercantiles debido a que es más rápido, más barato y en general más confiable. Pero siguen existiendo algunas aplicaciones de correo donde la copia papel sigue siendo predominante, como es el caso del correo certificado. Por ejemplo, cuando una carta es enviada por correo certificado, al remitente se le proporciona un acuse de recibo para probar que la carta fue enviada. Un recibo de correo certificado, retomado, agrega la confirmación del Servicio Postal que la carta fue satisfactoriamente entregada al destinatario o al agente autorizado del destinatario. Adicionalmente, correos privados tales como Federal Express® y United Parcel Service® (UPS), proporcionan algún tipo de confirmación de entrega. Ya que cada pieza de paquete de correo es, en efecto, registrada es natural que los consumidores acudan a esos servicios cuando desean una prueba de la entrega.

Muchos sistemas existentes de correo electrónico y programas de correo electrónico proporcionan ya alguna forma de prueba de entrega. Por ejemplo, algunos sistemas de correo electrónico hoy en día permiten que un remitente marque un mensaje con etiquetas de "solicitud de notificaciones". Tales etiquetas permiten que un remitente solicite notificación que el mensaje fue entregado y/o cuando el mensaje fue abierto. Cuando un remitente solicita notificación de entrega, el sistema de correo electrónico de Internet puede proporcionarle al remitente un acuse de recibo de correo electrónico que el mensaje fue entregado al servidor de correo o al buzón electrónico del destinatario. El mensaje de acuse de recibo puede incluir el titulo del mensaje, la dirección de destino y el tiempo de entrega. Este puede también incluir (dependiendo de los tipos de "indicadores" que son proporcionados y activados en el software de envío), una lista de todas las "estaciones" de Internet que el mensaje recorrió en ruta hacia su destino. Esta forma de informar está constituida dentro de algunas de las reglas y protocolos que implementan el correo electrónico. Además, cuando un mensaje es enviado con una solicitud de "notificación de lectura" el programa de correo electrónico del destinatario puede enviarle al remitente una notificación de correo electrónico indicando que el destinatario abrió ese mensaje para su lectura. Muchos clientes de correo electrónico pueden y de hecho apoyan este tipo de informe; sin embargo, los protocolos de Internet no hacen esto obligatorio.

Sin embargo, esto no significa que un correo electrónico enviado con una petición de notificación sea tan efectivo en todos sus aspectos como el correo certificado. Diversas personas certifican y registran las cartas debido a que desean obtener una prueba de entrega, por ejemplo, una prueba que puede ser utilizada en un procedimiento civil o criminal, o una prueba que satisfará a un supervisor o a un cliente o a una agencia gubernamental de que un mensaje ha sido enviado, una labor ha sido realizada, una orden colocada, o un requerimiento de contrato satisfecho.

Un recibo de registro del Servicio Postal de los Estados Unidos de América (USPS) constituye una prueba de la entrega debido a que el USPS se encuentra tras la misma. Un acuse de recibo representa la confirmación de la Oficina Postal que la carta o encomienda en cuestión fue efectivamente entregada al destinatario o a su representante autorizado. Por otra parte, con el acuse de recibo de correo electrónico existen diversos obstáculos para que un acuse de recibo de correo electrónico sea admitido y sirva de base como evidencia persuasiva en un tribunal de justicia, como una prueba que el mensaje fue entregado. Después de todo, el acuse de recibo podría ser solo otro mensaje de correo electrónico que podría haber sido alterado o creado por cualquiera, en cualquier momento.

Existe una necesidad de un sistema de correo electrónico y/o método que pueda proporcionar prueba confiable del contenido y entrega de un mensaje de correo electrónico, con el fin de sacar mejor provecho de la conveniencia y del bajo costo de la comunicación por correo electrónico.

Para cumplir esta necesidad, se han establecido algunos sistemas, mediante los cuales los remitentes pueden recibir una prueba de entrega de parte de un tercero, suscribiéndose a servicios mediante los cuales:

a) El remitente transmite un mensaje electrónico a un tercero junto con una lista de los destinatarios pretendidos del documento.

b) El tercero envía una notificación a cada uno de los destinatarios pretendidos del mensaje, invitándolos a visitar la página Web del tercero, donde se puede ver el mensaje.

c) Si el destinatario pretendido visita la página Web del tercero para ver el mensaje, el tercero registra esta

d) visita de modo que el remitente pueda saber que su mensaje ha sido leído por el destinatario.

Los inconvenientes de tales sistemas son múltiples. En primer lugar, éstos confían esencialmente en la cooperación del destinatario del correo electrónico para recolectar sus mensajes del servicio del tercero. Pero las circunstancias en las cuales un remitente puede desear una prueba de la entrega de un mensaje, son frecuentemente circunstancias en las cuales no se puede asumir que el destinatario pretendido cooperará en la recepción del mensaje. En los casos en que, por ejemplo, el acusar recibo del mensaje podría colocar una carga financiera o legal sobre el destinatario, éste último puede simplemente ignorar la notificación que hay un correo a su disposición, para recibir. Nótese que no existe nada en tal sistema para garantizar que el destinatario pretendido ha recibido la notificación de tener correo pendiente. En segundo lugar, tales sistemas son problemáticos y lentos para utilizarse comparado con el correo electrónico regular, en cuanto a que éste puede requerir que el remitente y/o el destinatario se conecten a un sitio Web de la Red Mundial (*World Wide Web*) para enviar, recolectar y verificar la entrega de cada mensaje. Además, la transmisión de documentos mediante tales métodos puede requerir que el remitente y el destinatario carguen y descarguen archivos desde o hacia un sitio de la red. Finalmente, debido a que estos métodos requieren que el tercero conserve una copia de la totalidad de cada mensaje hasta que éstos sean recolectados o hayan expirado, los métodos pueden requerir que su proveedor destine recursos computacionales sustanciales para el almacenamiento de datos y el rastreo de datos durante un periodo prolongado de tiempo. Como un método alternativo de proporcionar prueba de la entrega, algunos sistemas proporcionan a los clientes de correo electrónico propietarios o de buscadores de la red programas de extensión específicos (*plug-ins*) que notificarán a los remitentes cuando un mensaje ha sido recibido, siempre que que el destinatario utilice el mismo cliente de mensajería. La desventaja obvia de tales sistemas es que requieren que tanto el remitente come el destinatario utilicen el mismo cliente de mensajería.

Existe por lo tanto una necesidad para un sistema/método de correo electrónico que pueda proporcionar una prueba confiable del contenido y de la entrega de los mensajes electrónicos, que no requiera el cumplimiento o la cooperación del destinatario, que no requiera un software de correo electrónico especial por parte del remitente o del destinatario, que opere con la misma o casi la misma conveniencia y velocidad de uso que el correo electrónico convencional y que pueda ser operado económicamente por un proveedor de servicio.

Un objetivo general de la invención divulgada y reivindicada en solicitud co-pendiente no-provisional 09/626,577 (archivo de abogados RPOST-57228) presentado por Terrance Tomkow el 27 de Julio, 2000 y cedido de registro al cesionario de registro en esta solicitud, (subsecuentemente publicado como solicitud de patente internacional no. WO-A-02/1 1025), es proporcionar un sistema y método para una verificación confiable, a través de documentación segura y a prueba de alteraciones, el contenido y entrega de un mensaje electrónico tal y como un correo electrónico. Esta solicitud representa conocimiento previo de conformidad con lo dispuesto en la Regla 29(1)(a). Idealmente, la invención divulgada y reivindicada en la solicitud co-pendiente 09/626,577 (archivo de abogados RPOST-57228) proporcionará al correo electrónico y otros mensajes electrónicos un estatus legal igual, o incluso superior, al correo registrado de los Estados Unidos de América. Sin embargo, no es necesario para la invención que se establezca algún estatus legal particular para los mensajes enviados según los métodos expuestos aquí, puesto que la invención proporciona información útil y verificación independientemente de ello.

La invención divulgada y reivindicada en la solicitud co-pendiente no-provisional 09/626,577 incluye un sistema de mensajes electrónicos que crea y registra una firma digital de cada mensaje electrónico enviado a través del sistema. Un autor puede enviar una copia del mensaje de correo electrónico al sistema o generar el mensaje electrónico dentro del mismo sistema. El sistema, entonces, redirige y entrega el mensaje electrónico a todos los destinatarios (o a los gestores de correo designados asociados con los destinatarios), incluyendo destinatarios "A" ("*to*") y destinatarios "cc". A partir de ese momento, el sistema devuelve un recibo de entrega al creador del mensaje electrónico. El recibo incluye, entre otras cosas: el mensaje original, la firma digital del mensaje y un historial de la sincronización de reconocimiento e intercambio (*handshaking*) y de la entrega, incluyendo los tiempos de entrega a los destinatarios. Para verificar y autenticar posteriormente la información contenida en el recibo, el creador o usuario envía una copia del recibo al sistema. El sistema verifica en ese momento que la firma digital coincida con el mensaje original y el resto del recibo. Si ambos coinciden, el sistema envía entonces una carta o proporciona otra confirmación de autenticidad verificando que el mensaje electrónico no ha sido alterado.

El sistema divulgado y reclamado en solicitud co-pendiente no-provisional 09/626,577 puede incluir un tipo de servidor de correo electrónico conectado a Internet, que puede ser utilizado de varias maneras. Por ejemplo, los usuarios individuales pueden registrar sus mensajes electrónicos, como correos electrónicos, enviando una "copia carbón" (cc:) al sistema o redactando el mensaje dentro del sistema mismo. Los usuarios corporativos o de comercio electrónico, pueden cambiar su servidor a un servidor que incorpora la presente invención y hacer todos sus mensajes electrónicos externos sean registrados, con la opción de hacer que el sistema conserve y archive los recibos. El sistema puede aceptar y verificar mensajes electrónicos encriptados y administrar los mensajes electrónicos delante o detrás de un "cortafuegos" (*fire wall*). Los usuarios situados en la Web, por ejemplo, individuos o corporaciones que utilizan correos electrónicos situados en la Web (Webmail), como MSN Hotmail® o Yahoo Mail®, pueden seleccionar una casilla o sino incluir un indicador dentro de sus programas de correo electrónico para seleccionar caso por caso si hacer los correos electrónicos de registro y/o archivar los mensajes utilizando el sistema divulgado y reclamado en la solicitud co-pendiente no-provisional 09/626,577.

La firma digital puede ser creada utilizando técnicas de firma digital conocidas, tales como realizar una función de hash sobre el mensaje para producir un digesto de mensaje y luego cifrando el digesto de mensaje. Se pueden crear firmas digitales separadas para el cuerpo del mensaje, cualquier archivo adjunto y para la totalidad del mensaje, incluyendo el cuerpo, los archivos adjuntos y los digestos individuales de cada mensaje. El digesto de mensaje encriptado proporciona un tipo de autenticación de mensaje o código de validación o documentación segura. Se puede también generar y utilizar otra autenticación de mensaje y/o códigos de validación.

La patente de Estados Unidos de América no. 6,314,454 describe un sistema que permite a los usuarios enviar mensajes certificados de correo electrónico. Un servidor recibe un mensaje de correo electrónico designado para entrega certificada. El servidor dirige el mensaje de correo electrónico a una cuenta receptora. Cualquier acción tomada con respecto al mensaje por la cuenta receptora es transmitida al servidor, que envía dicha información al remitente.

La patente de Estados Unidos de América no. 6,343,313 describe un sistema de comunicaciones de computadoras interconectadas que maneja flujos de datos arbitrarios y transporta a diferentes velocidades dichos flujos, donde actualizaciones intermedias pueden ser descartadas si las mismas se tornan obsoletas por actualizaciones de datos entrantes posteriores, optimizando la utilización de recursos de red y nodo, el mensaje electrónico; y proporcionando al remitente del mensaje, como mínimo, una parte del dialogo SMTP y por lo menos una parte de la información de DSN.

En todavía otro aspecto, la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577 incluye un método para verificar el contenido de un mensaje electrónico recibido, incluyendo: recibir el mensaje electrónico; generar una firma digital correspondiente al contenido del mensaje recibido; proporcionar el mensaje y la firma digital a un destinatario designado; y, posteriormente, verificar que la firma digital corresponda al mensaje.

De acuerdo con aun otro aspecto de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577, el método incluye establecer si un mensaje fue recibido electrónicamente por un destinatario, incluyendo: probar que un mensaje fue despachado electrónicamente junto con la dirección de un destinatario de parte de un remitente; crear una firma asociada al mensaje; despachar el mensaje por vía electrónica a la dirección del destinatario; rastrear el mensaje para determinar un Estado de Entrega final del mensaje despachado a la dirección del destinatario; tras recibir el Estado de Entrega final del mensaje, generar un recibo, el recibo incluyendo una copia del mensaje, la firma y el Estado de Entrega final para el mensaje; y proporcionar el recibo al remitente para establecer posteriormente que el mensaje fue recibido electrónicamente por el destinatario.

De acuerdo con aun otro aspecto de la invención divulgada y reivindicada en solicitud co-pendiente 09/626, 577, se proporciona un método para demostrar que un mensaje electrónico enviado a un destinatario fue leído, incluyendo: proporcionar un mensaje electrónico junto con una dirección de destinatario; calcular una firma digital que corresponda al mensaje electrónico; despachar el mensaje por vía electrónica a la dirección del destinatario; solicitar una notificación (de "lectura") del destinatario a un Agente de Usuario de Correo (*Mail UserAgent*) (cliente de correo electrónico) del destinatario; tras recibir la notificación de lectura, generar un recibo de lectura, el recibo de lectura incluyendo una copia del mensaje, la firma digital para el mensaje electrónico correspondiente y una segunda firma digital para el recibo de lectura del destinatario; y proporcionar el recibo de lectura para posterior verificación que dicho mensaje fue recibido por el destinatario.

De acuerdo con otro aspecto de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577, se proporciona un método para validar la integridad de la copia aparente de un mensaje electrónico, incluyendo: recibir la copia aparente del mensaje electrónico, dicha copia aparente incluyendo un digesto de mensaje cifrado asociado con este; descifrar el digesto de mensaje; generar un segundo digesto de mensaje basado en el contenido de la copia aparente; y validar la copia aparente al comparar el digesto de mensaje descifrado y el segundo digesto de mensaje para determinar si los dos digestos de mensaje concuerdan.

De acuerdo con aspectos aun mas allá de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577, se proporciona un método para la validación de un correo electrónico registrado recibido, incluyendo: recibir un recibo electrónico, dicho recibo incluyendo un mensaje de base y un digesto de mensaje cifrado; descifrar el digesto de mensaje cifrado; generar un segundo digesto de mensaje a partir del mensaje de base; y validar el correo electrónico si el digesto de mensaje cifrado concuerda con el segundo digesto de mensaje.

En aun otro aspecto, la invención divulgada y reivindicada en solicitud co-pendiente 091626,577 incluye un sitio Web en el cual los usuarios tienen la posibilidad de acudir para enviar y recibir mensajes seguros, el anfitrión del sitio Web (*website host*) desempeñándose como tercero independiente, que enviará y recibirá los mensajes y proporcionará documentación segura con respecto al contenido y a la entrega de los mensajes.

Los objetivos antes descritos de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577 y otras características y beneficios de la presente invención, se tornarán evidentes para aquéllos expertos en la materia cuando se lean conjuntamente con la siguiente descripción detallada de una personificación preferida ilustrativa y cuando sean vistos conjuntamente con los dibujos adjuntos en los cuales los mismos números de referencia corresponden a los mismo números de las partes, así como las reivindicaciones añadidas.

Breve descripción de las personificaciones preferidas de la invención

La presente invención proporciona un método para transmitir un mensaje de un remitente a una dirección de destino de acuerdo a la reivindicación 1.

En términos generales, un servidor recibe un mensaje de parte de un remitente y transmite el mensaje a través de Internet al destinatario. El servidor normalmente transmite el mensaje en una primera ruta por Internet hacia el destinatario. Cuando el remitente indica en una posición particular en el mensaje que el mensaje es registrado, el servidor transmite el mensaje por una segunda ruta vía Internet hacia el destinatario. El remitente también puede proporcionar indicaciones adicionales en el mensaje para hacer que el servidor maneje el mensaje en otras formas especiales que normalmente no son proporcionadas por el servidor.

Después de enterarse por el recibo o a través del agente del destinatario vía Internet que el mensaje fue satisfactoriamente recibido, el servidor crea y manda al remitente, un recibo electrónico. El recibo incluye por lo menos uno y preferiblemente la totalidad, de: el mensaje y cualquier archivo adjunto, una plantilla de éxito/fracaso de la entrega, detallando los recibos y la fecha y hora de recepción del mensaje por parte de los agentes específicos de destinatario y el fracaso de otros agentes del destinatario para recibir el mensaje así como una firma digital del mensaje y archivos adjuntos subsecuentemente. Al verificar que la firma digital en el recibo del remitente concuerda con el recibo digital en el servidor, el servidor puede verificar, sin retener el mensaje, que el recibo es genuino y que el mensaje es exacto.

Breve descripción de los dibujos

Una detallada descripción de la personificación preferida de la invención será hecha con referencia a los dibujos acompañantes:

La Fig. 1 es un diagrama de sistema de una primera personificación de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577, según la cual los mensajes salientes son registrados al ser transmitidos por un Agente de Transporte de Correo (*Mail Transport Agent*) (MTA) especial.

Las Figs. 2-2F constituyen un diagrama de flujo representativo para hacer de registro un correo electrónico saliente de acuerdo a la personificación de La Fig. 1.

La Fig. 3 es un diagrama de sistema de una segunda personificación de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577, en cuya personificación los remitentes pueden instruir a un Agente de Transporte de Correo para que transmita los mensajes seleccionados a través de un Agente de Transporte de Correo diseñado para hacer de registro los mensajes seleccionados.

La Fig. 4 es un diagrama de sistema de una tercera personificación de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577, en la cual se envían copias carbón (cc's) de los mensajes salientes a un servidor especial para hacerlos de registro.

La Fig. 5 es un diagrama de sistema de una cuarta personificación de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577, según la cual los usuarios componen mensajes salientes para hacerlos de registro en un sitio web designado.

La Fig. 6 es un diagrama de sistema de una quinta personificación de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577 en la cual los usuarios pueden enviar correos electrónicos hechos de registro y archivar recibos dentro de un Agente de Usuario de Correo (*Mail User Agent*) (MUA) situado en la Web.

La Fig. 7 es un diagrama de flujo para validar un recibo de correo electrónico hecho de registro.

La Fig. 8 es un diagrama de sistema de una personificación de la presente invención para hacer de registro los mensajes entrantes.

La Fig. 9 es un diagrama de flujo para hacer de registro los mensajes entrantes.

La Fig. 10 es un diagrama de flujo para validar mensajes recibidos hechos de registro.

La Fig. 11 es un diagrama de sistema representando un uso ejemplar de la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577 por parte de un comercio electrónico para hacer de registro y confirmar las comunicaciones entrantes y salientes.

La Fig. 12 es un diagrama de bloques representando un gráfico de flujo de un método para hacer de registro el correo en un sistema como el representado en las diferentes personificaciones individuales mostradas en las Figuras previas y mostrando como un mensaje de un remitente a un servidor, con una indicación representando correo hecho de registro, provee la transmisión del mensaje por parte del servidor a un destinatario a través de una ruta especial distinta de la ruta por la cual el mensaje es normalmente transmitido por parte del servidor hacia el destinatario;

La Fig. 13 es un diagrama de bloques representando un gráfico de flujos similar al mostrado en Figura 12 pero con bloques adicionales para proporcionar funciones especificas adicionalmente a las funciones proporcionadas por el gráfico de flujos en la Figura 12; y

La Fig. 14 es una vista parcial de una forma utilizada por el remitente para hacer de registro un mensaje que será enviado por el servidor al destinatario.

Descripción detallada de las personificaciones preferidas de la invención

Esta descripción no debe ser tomada en un sentido limitativo, sino que está hecha meramente con el propósito de ilustración de los principios generales de la invención. Los títulos de sección y la organización general de la presente descripción detallada tiene como único propósito el de conveniencia y no tienen la intención de limitar la presente invención. Acordemente, la invención será descrita con respecto a sistemas de mensajería de correo electrónico que utilizan la arquitectura y la infraestructura de red de Internet. Debe comprenderse que el tipo particular de mensaje y de arquitectura de red descrita aquí es para ilustración únicamente; la invención también se aplica a otros protocolos de mensaje electrónico y tipos de mensaje que utilizan otras arquitecturas de red de computadoras, incluyendo redes alámbricas e inalámbricas. Para conveniencia de discusión, los mensajes que son procesados de acuerdo a la invención divulgada y reivindicada en solicitud co-pendiente 09/626,577 serán designados aquí como mensajes "hechos de registro". En la descripción a continuación, el término "RPost" se referirá en términos generales a una entidad de terceros que crea y/u opera software y/o hardware implementando la presente invención y/o actúa como tercero desinteresado verificador de mensaje. Los mensajes que son procesados según las presentes invenciones son designados como mensajes "registrados". El término es utilizado para conveniencia de discusión ejemplar únicamente y no debe entenderse como limitativo de la invención.

Personificación de RPost como servidor de correo saliente

La Fig. 1 es un diagrama de sistema de una primera personificación de la presente invención, donde correos electrónicos salientes son hechos de regtstrp de acuerdo a la invención divulgada y reivindicada en solicitud co-pendiente no-provisional 09/626,577. En esta personificación, el servidor RPost 14 sirve como Agente de Transporte de Correo (MTA) saliente principal para un mensaje de remitente Agente de Usuario de Correo (MUA) 13. Aunque el destinatario del mensaje 18 es técnicamente el destinatario y por lo tanto simplemente el destinatario pretendido o destino pretendido en ese momento, para simplicidad de la discusión esta entidad se denominará aquí como el destinatario o destino. Nótese que un mensaje individual puede tener muchos destinos distintos y que cada uno de estos puede ser alcanzado a través de un MTA distinto. El método para enviar mensajes hechos de registro puede dividirse en tres partes:

1) Pre procesamiento: los pasos a realizarse antes de transmitir un mensaje;

2) Transmisión: el método para entregar mensajes a los destinatarios;

3) Post procesamiento: los procedimientos para obtener información sobre los mensajes después de su entrega, la creación de recibos y la validación de recibos.

1.1 *Pre procesamiento*

Al recibir un mensaje para su transmisión, el servidor RPost 14 creará registros en una base de datos para cada mensaje que se utilizará para almacenar información como:

a) el tiempo en el cual el mensaje fue recibido;

b) los nombres de los archivos adjuntos del mensaje; y

c) el número de direcciones del mensaje.

Para cada destino del mensaje, la base de datos registrará:

a) el nombre del destino (si está disponible);

b) la dirección de Internet del destino;

c) el tiempo en el cual el mensaje fue entregado al Servidor de Correo de destino; y

d) el *Estado de Entrega* de este destino.

Los Estado de Entrega del Destinatario utilizados por el sistema incluirán:

NO ENVIADO

Este estado indica que el mensaje no ha sido enviado.

ENTREGADO-Y-EN ESPERA-DEL-DSN

Este estado indica que el mensaje ha sido entregado a un MTA compatible con ESMTP que soporta la Notificación de Estado de Entrega (*Delivery Status Notification*) (DSN) de forma tal que se pueda esperar una notificación de éxito/fracaso.

ENTREGADO

Este estado significa que la copia del mensaje enviado a este destinatario ha sido satisfactoriamente entregada a un servidor que no soporta DSN ESMTP.

ENTREGADO-A-CASILLA DE CORREO

Este estado significa que un mensaje DSN ha sido recibido indicando que la copia del mensaje enviado a este destinatario fue entregada a la casilla de correo del destinatario.

REENVIADO

Este estado significa que un DSN de MTA ha sido recibido indicando que la copia del mensaje enviado a este destinatario ha sido reenviada hacia otro servidor.

NO-ENTREGABLE

Este estado indica que después de múltiples intentos RPost no ha podido conectarse con un MTA para entregar los mensajes al destinatario.

FRACASO

Este estado significa que un DSN de MTA ha sido recibido indicando un fracaso en entregar una copia del mensaje a este destinatario.

En este momento el sistema también llevará a cabo funciones de hash en los contenidos del mensaje.

El servidor RPost 14 emplea una función de hash y un algoritmo de cifrado. La función de hash puede ser una de cualesquiera funciones de hash conocidas, incluyendo MD2, MD5, el Algoritmo de Hash Seguro (*Secure Hashing Algorithm*) (SHA), u otras funciones de hash que podrían ser desarrolladas en el futuro. Los algoritmos y métodos de Hash son descritos en Criptografía Aplicada: Protocolos, Algoritmos y Código Fuente en C de Bruce Schneider, (*Applied Cryptography: Protocols, Algorithms, and Source Code in C*), publicado por John Wiley & Sons, Inc. (New York) 1993; la Publicación de Estándar de Procesamiento de Información Federal (*Federal Information Processing Standard Publication*) 180-1 (FIPS PUB 180-1), el Estándar de Hash Seguro (*Secure Hash Standard*), Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*); y en la Patente de los Estados Unidos de América No. 5,530,757 emitida a Krawczyk, titulado "Huella Digital Distribuida para Verificación de Integridad de Información" ("*Distributed Fingerprints for Information Integrity Verification*") que enseña funciones de hash, de cifrado y métodos y sistemas para implementar esas funciones. Pueden utilizarse otros métodos conocidos o nuevos para detectar si los contenidos del mensaje han sido alterados.

Una buena función hash H es unidireccional; es decir, que es difícil de invertir, cuando "difícil de invertir" significa que dado un valor h hash, es computacionalmente imposible encontrar una entrada x en modo que H(x) = h. Además, la función de hash debe ser, como mínimo, débilmente libre de colisión, lo que significa que, dado un mensaje x, es computacionalmente imposible encontrar una entrada y en modo que H(x) = H(y). La consecuencia de esto es que un potencial falsificador que conoce el algoritmo utilizado y el valor hash resultante o el digesto de mensaje no puede sin embargo crear un mensaje falso, cuyo hash coincida con el mismo número. El valor hash h devuelto por una función de hash es generalmente llamado un digesto de mensaje. El digesto de mensaje es algunas veces designado "huella digital" del mensaje x. Actualmente, se recomienda que las funciones de hash unidireccionales produzcan un resultado que sea por lo menos de 128 bits de largo, con el objetivo de asegurar que los resultados sean seguros y no falsificables.

Al paso al que evoluciona el presente estado de la técnica, la longitud recomendada para las funciones de hash seguras podría incrementar.

El servidor Rpost 14 computa un digesto de mensaje para el cuerpo de mensaje y un digesto de mensaje separado para cada uno de los archivos adjuntos del mensaje y conserva los mismos de forma tal que puedan ser incluidos posteriormente en un recibo del mensaje.

Antes de que el mensaje sea alterado por los requerimientos propios del registro, una copia del mensaje original y sus archivos adjuntos son almacenados de un modo que permita que los mismos pueden ser recuperados posteriormente por el sistema.

El servidor Rpost 14 puede alterar un mensaje de múltiples formas antes de la transmisión al MTA del destinatario.

Aunque dicho procedimiento no es necesario para la práctica de la invención, el mensaje puede ser etiquetado para denotar el hecho que el mensaje ha sido hecho de registro, como por ejemplo incluyendo las palabras “Hecho de Registro” o aplicando al inicio de la línea “asunto” del mensaje una etiqueta como:

“Este mensaje ha sido hecho de registro con RPost. Visite nuestro sitio Web en la dirección www.RPost.com para información adicional”. Al final de los mensajes originales u otro tipo de etiquetas.

Adicionalmente, la etiqueta puede contener instrucciones, direcciones de la Red Mundial de Internet (*World Wide Web*) o vínculos que invitan y permiten al destinatario enviar una respuesta hecha de registro al mensaje vinculándose a una Página Web desde la cual pueden redactarse y enviarse mensajes hechos de registro.

Si bien el etiquetado es opcional, el mensaje entregado será generalmente designado aquí el mensaje etiquetado.

Los protocolos de Internet proporcionan dos formas de recibo para mensajes de correo electrónico:

Notificaciones MTA

Estos son correos electrónicos que son enviados por el MTA del destinatario, notificando al remitente nominal del mensaje que varios eventos han ocurrido. Los MTAs que se ajustan al protocolo SMTP normalmente solo enviarán una notificación en el caso de que el agente de correo no puede entregar un mensaje a la casilla de correo del destinatario (como puede suceder si la dirección no es válida o si la casilla de correo del destinatario ha excedido su cuota de almacenamiento permitida).

Con la introducción del estándar SMTP Extendido se ha vuelto posible para los MTAs remitentes solicitar notificaciones de éxito y fracaso de la entrega de los mensajes. Esas Notificaciones de Estado de Entrega (DSN) son correos electrónicos enviados por un MTA receptor al remitente nominal del mensaje cuando ocurren ciertos eventos: por ej. El mensaje ha sido satisfactoriamente depositado en la casilla de correo del destinatario; el mensaje no puede ser entregado a la casilla de correo del destinatario por alguna razón; el mensaje del destinatario ha sido reenviado a otro servidor que no proporciona recibos DSN.

Nótese que solamente los servidores de correo electrónico que soportan el protocolo SMTP Extendido (ESMTP) soportan esta forma de DSN y que el soporte para esta función es opcional para servidores ESMTP y depende de la configuración seleccionada por el administrador del servidor.

A pesar de que DSN es un término que solamente se empezó a usar con el advenimiento del ESMTP, a continuación usaremos “DSN” para referirnos a cualquier mensaje generado por un MTA que se refiera al estado de un mensaje recibido, sea éste conforme o no al protocolo ESMTP.

Notificaciones MUA (Notificaciones de lectura)

Estos son correos electrónicos que son enviados al autor (nominal) de un mensaje por el Agente de Usuario de Correo (MUA) (programa de correo electrónico) del destinatario cuando ocurren ciertos eventos: por ej. el mensaje es abierto para su lectura, o borrado del sistema sin ser leído. Por la convención de Internet (RFC 1891), ningún programa MUA puede ser obligado a generar dichas notificaciones. El que un MUA llegue a generar dichos recibos va a depender de la configuración seleccionada por su usuario.

El servidor Rpost 14 configurará y transmitirá mensajes de una forma que intentará obtener ambas notificaciones DSN de MTA y MUA de los MTAs y MUAs compatibles. Para obtener un Recibo de Lectura de MUAs compatibles, deberán incluirse ciertos encabezados en la sección de encabezado de un mensaje de correo electrónico. Distintos MUAs responden a distintos encabezados; por lo tanto, el Servidor 14 deberá agregar diferentes encabezados a cada mensaje que solicite una notificación de lectura de una forma reconocida por varios MUAs. Estos encabezados toman todos la siguiente forma:

Etiqueta de encabezado: nombre de usuario <dirección de usuario>

Por ejemplo:

Disposición–notificación-a: john smith

<jsmith@adomain.com>

Notificación-de lectura-a: john smith

<jsmith@adomain.com>

en el cual "john smith" es el nombre del usuario a quien una notificación MUA debe ser enviada y "<jsmith@adomain.com>" es la dirección de Internet de este usuario. Normalmente, dichos encabezados se referirían al autor del mensaje pero en el caso del presente método, se requiere que la notificación sea devuelta a RPost de forma tal que la notificación pueda ser procesada por RPost. Para asegurarse de que éste sea el caso, el Servidor 14 insertará encabezados que soliciten que los recibos MUA sean enviados a una dirección donde puedan ser procesados por el servidor RPost, por ejemplo: "readreceipts@RPost.com". Esto le indicará a cualquier MUA receptor compatible que envíe sus notificaciones a una dirección RPost para su procesamiento.

La tarea de procesar notificaciones MUA devueltas hace surgir otro problema que debe ser resuelto en esta etapa. No existen estándares que gobiernen el formato o el contenido de las notificaciones MUA. A menudo harán referencia al titulo o al asunto del mensaje original y a la hora del evento (por ej. "abierto para lectura") que están reportando. Pero aunque esta información esté incluida en la notificación es raramente suficiente para identificar como único al mensaje que lo provoca o para identificar al autor de ese mensaje. Cuando el sistema recibe una notificación MUA debe contar con la capacidad de identificar al mensaje que lo provoca, de tal manera que pueda incluir la información de la notificación en el recibo que RPost generará para el remitente. Alternativamente, el sistema debería, por lo menos, ser capaz de identificar en modo confiable al remitente de mensaje al cual hace referencia la notificación MUA, de forma tal que la información de la notificación pueda ser transmitida al remitente en forma de un recibo de Lectura de RPost (ver más abajo).

Para cumplir con este último objetivo, el sistema puede sacar provecho del hecho que las direcciones Internet tienen dos componentes: un campo 'nombre' y un campo 'dirección', el campo 'dirección' estando delimitado por cuñas "<>". La mayoría de los MUAs incluirán ambos campos en la dirección de destino de sus notificaciones MUA. Al componer sus solicitudes de recibos MUA, el sistema RPost incluirá la dirección de manejo-de-recibo del servidor 14 como la dirección para la notificación pero utilizará la dirección del remitente original en el campo 'nombre' del encabezado. Por ejemplo, si el remitente original del mensaje es el usuario John Smith con dirección de Internet jsmith@domain.com, el servidor Rpost 14 incluirá encabezados de la siguiente forma:

Disposición-notificación-a: jsmith@adomain.com

<read receipts@RPostcom>

Esto típicamente resultará en que el MUA compatible envíe una notificación a readreceipts@RPost.com señalada como:

jsmith@adomain.com <readreceipts@RPost.com>

Al recibir dicha notificación en la dirección "readreceipts@RPost.com", el servidor puede, analizando el campo de destinatario, determinar que la notificación concierne un mensaje originalmente enviado por jsmith@adomain.com, por más que esto no pueda ser determinado examinando los contenidos de la notificación. Con esta información en mano, el servidor puede empaquetar los contenidos de la notificación en un recibo de Lectura RPost digitalmente firmado y enviar el recibo a la dirección jsmith@adomain.com.

El sistema RPost también intentará por todos los medios obtener y recoger notificaciones DSN de MTA generadas por los MTAs del destinatario. Puesto que dichas notificaciones son siempre enviadas a la dirección referida en el campo "DE:" ("*FROM*:") del encabezado del mensaje, el servidor 14 alterará cada encabezado de mensaje de forma tal que el mensaje es recibido como "DE:" una dirección RPost en la cual los DSN pueden ser procesados.

Sin embargo, el problema de procesamiento de DSN plantea otra cuestión, que será resuelta en esta etapa. Los DSN no tienen ningún estándar de contenido o formato; a menudo es imposible determinar, simplemente examinando los contenidos de esos correos electrónicos, cual es el mensaje que están notificando sus contenidos. Este problema supuestamente se refería a los DSN generados en compatibilidad con el protocolo ESMTP mediante el uso de números de identidad (ver RFC 1869) de sobre DSN (*envelope ID numbers*). Según el protocolo, un MTA transmisor puede incluir un número de referencia junto a su solicitud de DSN. Este número seria mencionado en cualquier DSN devuelto, permitiendo al remitente identificar el asunto del mensaje del DSN. Sin embargo, de hecho, muchos MTAs que se reportan a sí mismos como soportando DSN ESMTP no devuelven una identidad de sobre DSN ni cualquier otra información suficiente para identificar de manera confiable el asunto de mensaje. Finalmente, aun cuando un DSN realice la devolución de información suficiente para identificar el mensaje del cual está proporcionando notificación, a menudo no contendrá información suficiente para identificar el destinatario específico del mensaje que ha generado la

notificación. Por lo tanto, un único mensaje puede ser enviado a dos destinatarios en mismo dominio; uno puede ser satisfactoriamente entregado a la casilla de correo del destinatario; el otro, no. El MTA para el dominio puede informar esos eventos en un DSN en modos que no proporcionan al remitente una forma de determinar a cual destinatario le fue satisfactoriamente entregado y a cual no (como por ejemplo, puede suceder si los DSN reportan la dirección del destinatario por sus nombres o alias locales en lugar de hacerlo por la dirección contenida en el mensaje original).

La presente invención soluciona este problema en cuatro pasos:

1) Un número de identificación único es generado por cada mensaje saliente (por ej. basado en un sello de tiempo). Este número es almacenado en una base de datos.

2) Los destinatarios de cada mensaje son enumerados y los números de identificación almacenados en una base de datos.

3) El mensaje es enviado separadamente al MTA de cada uno de los destinatarios pretendidos. (Aun cuando dos destinatarios tengan un nombre de dominio y MTA común, el servidor 14 transmitirá el mensaje a ese MTA en dos sesiones SMTP de telnet separadas).

4) Cuando el servidor 14 transmite el mensaje a un MTA de destinatario, aumenta el espacio "DE" del mensaje para mostrar el mensaje como habiendo sido enviado desde una dirección que incorpora la identidad única del mensaje y el número de identificación del remitente. La dirección también contiene una subcadena (por ej. "rcpt") que habilita al servidor para identificar mensajes de retorno como DSNs.

Por lo tanto, un único mensaje denominado "mmyyddss" por parte del servidor 14, del remitente llamado John Smith, podrá ser enviado a su primer destinatario pretendido (denominado "a" por el sistema) con un encabezado que lee:

De: John Smith rcptmmddyyssb@RPost.com

El mismo mensaje podría ser enviado al Segundo destinatario con un encabezado que lea:

De: John Smith <rcptmmddyyssb@RPost.com>

Muchos MUAs de correo electrónico desplegarán únicamente el nombre del remitente de un mensaje y por lo tanto la dirección especial no será visible para la mayoría de los destinatarios.

La ventaja de esta forma de mandar es que cuando los MTAs del destinatario emiten DSNs (sean o no compatibles ESMTP) ellos mandarán esos DSNs a distintas direcciones RPost. Cuando recibe esos DSNs, el servidor 14 puede identificarlos como mensajes DSN por su prefijo "RCPT" y, al analizar los destinatarios, puede determinar cual mensaje y cual destinatario es el tema del DSN.

El servidor 14 alterará el campo "DE" de cada mensaje para referirse a un destinatario del mensaje cada vez que intente transmitir el mensaje al MTA de ese destinatario

Para asegurar que las respuestas del destinatario a los mensajes transmitidos sean dirigidas adecuadamente el servidor 14 agregará un encabezado de mensaje explícito "responder-a:" ("*reply-to*:") en el mensaje que incluye el nombre del remitente original y la dirección Internet. En el caso del presente ejemplo este sería:

Responder-a: John smith <jsmith@adomain.com>

Esto guiará a los MUAs del destinatario a mandar las respuestas a un mensaje recibido a la dirección real del remitente, en lugar de la dirección construida por RPost.

1.2 *Transmisión*

Como fue señalado más arriba, es parte del método que el servidor 14 transmita una copia separada de un mensaje saliente a cada destinatario de ese mensaje. Además, RPost intentará realizar cada una de dichas entregas a través de una conexión directa de SMTP con un intercambiador de correo (mail eXchanger) (MX) de registro para cada destino.

Aviso: cada dirección válida de correo electrónico de Internet incluye un nombre de dominio de Internet o una dirección IP. Cada nombre/dirección de dominio tiene asociado con el mismo un(os) servidor(es) de correo electrónico autorizado(s) a recibir correo para direcciones en ese dominio. Obsérvese que ciertos dominios tienen más de un servidor. El Servidor de Nombre de Dominio responsable para cada dominio difunde la identidad de sus servidores de correo a través de Internet. Esta información es de dominio público y es administrada y transmitida en formas que cumplen con las reglas y convenciones que gobiernan el correo electrónico y el servicio de Nombre de Dominio de Internet.

Antes de transmitir una copia de un mensaje a cualquier destino, el servidor Rpost 14 realizará una Consulta de Nombre de Servidor de Internet (*Internet Name Server Lookup*) para identificar un MTA asociado con el dominio de destino. Habiendo identificado el MTA responsable para recibir correo a nombre de una dirección de destino, el sistema intentará abrir una conexión telnet con el MTA local de destino.

Es una práctica común que los correos electrónicos de Internet sean reenviados de MTA en MTA hasta que alcancen su destino final. El propósito primordial para proporcionar una conexión directa entre el servidor Rpost 14 y el MTA de destino es que el servidor RPost pueda registrar la entrega del mensaje, (este registro toma la forma de un dialogo SMTP) con el servidor de correo electrónico que tiene la responsabilidad propietaria para recibir correo electrónico del nombre de dominio del destinatario.

La existencia de este registro proporciona evidencia útil que el mensaje fue entregado, de la misma forma que un recibo de correo registrado proporciona evidencia de entrega. El correo Registrado de USPS es considerado demostrablemente entregado si puede probarse que fue entregado al agente autorizado del destinatario (por ej. una secretaria o un funcionario del departamento de correspondencia). En el caso de algún desafío legal al mérito probatorio de un recibo de entrega RPost, deberá reconocerse que al seleccionar un proveedor de servicio de correo electrónico de Internet, el destinatario ha autorizado a ese proveedor a recolectar mensajes electrónicos a nombre suyo. A su vez, ese proveedor de servicio ha reconocido su estatus de agente autorizado para destinatarios de correo electrónico de ese nombre de dominio al difundir las direcciones de sus MTAs como los servidores de correo electrónico receptivos para este dominio.

Por consiguiente, al haber entregado los mensajes directamente al servidor de correo responsable para la recepción del correo electrónico del destinatario, RPost habrá entregado el mensaje a un agente que el destinatario ha autorizado legalmente a recibir su correo. Al registrar la transacción de entrega (esa transacción representada en la forma de un diálogo SMTP) RPost puede reivindicar contar con prueba de entrega al agente autorizado del destinatario.

Nótese que mientras que el método aquí descrito intenta recolectar otras formas de prueba de entrega para cada destino, sean o no exitosos estos intentos, va a depender de factores que no estarán bajo el control de RPost, (por ej. la forma de soporte SMTP utilizada en el servidor de correo del destinatario). Por otra parte, cada entrega exitosa directa a un servidor de correo de un destinatario siempre generará un registro SMTP. Registrar este registro le permite a RPost proporcionar prueba de la entrega a cualquier destino válido de Internet que cumple con los protocolos mínimos (SMTP) para el correo de Internet. Esto representa una importante ventaja del método actual sobre otros métodos que pueden intentar probar la entrega recurriendo a DSN de ESMTP.

Habiendo identificado al MTA para un destino de un mensaje, el servidor Rpost 14 intentará abrir una conexión ESMTP con el MTA de destino emitiendo un comando "EHLO" (*handshake*) en cumplimiento con RFC 1869. Si el SERVIDOR 16 soporta el ESMTP, este responderá listando cuales servicios ESMTP soporta el mismo.

Si el SERVIDOR 16 soporta el ESMTP, el servidor Rpost 14 determina en primer lugar si el SERVIDOR 16 soporta el Servicio ESMTP "VERIFICAR" ("*VERIFY*"). El servicio *Verificar* le permite a un servidor SMTP de llamada determinar, entre otras cosas, si una dirección en un dominio de MTA es genuina. Si el servidor Rpost 14 determina por esos medios que la dirección a la que está intentando entregar su mensaje no es válida, terminará la conexión, cesará los intentos de entregar un mensaje a este destinatario y registrará, en su base de datos, el estado de este destino de mensaje como NO-ENTREGABLE.

Cualquiera sea su resultado, el servidor Rpost 14 registrará el diálogo ESMTP "VERIFICAR" en un archivo y lo almacenará de forma tal que pueda ser adjuntado o incluido posteriormente en el Recibo de Entrega para este mensaje. Debe notarse que, debido a cuestiones de seguridad, pocos servidores ESMTP soportan la función VERIFICAR.

Si el Sistema 16 no soporta el método VERIFICAR, entonces el servidor Rpost 14 intentará sin embargo entregar el mensaje al Sistema 16. Normalmente, un MTA acepta mensajes para cualquier. dirección nominalmente en su dominio y envía ulteriormente un DSN si la dirección es inválida.

El servidor Rpost 14 intentará entonces determinar si el servidor de destino soporta DSN de servicio ESMTP. Si lo hace, RPost transmitirá el mensaje solicitando que el SERVIDOR 16 notifique el remitente del mensaje con un DSN ESMTP si la entrega al destinatario es exitosa o fracasa. Después de la transmisión exitosa del mensaje a este destino, el sistema registrará el Estado de Entrega de este destino como ENTREGADO-EN-ESPERA-DE-DSN.

Si el Servidor 16 responde al comando "EHLO" de forma tal que indique que no soporta el ESMTP, el servidor Rpost 14 emitirá un mensaje "HELO" para iniciar una conexión SMTP. Si esta conexión es lograda, el servidor Rpost 14 transmitirá el mensaje en cumplimiento con el protocolo SMTP y registrará el Estado de Entrega del destino como ENTREGADO.

Sea la conexión SMTP o ESMTP, el servidor Rpost 14 registrará la totalidad del diálogo de protocolo entre los dos servidores. Típicamente, este dialogo incluirá mensajes de protocolo en los cuales, entre otras cosas, el servidor de destino se identifica, otorga permiso para descargar un mensaje para un destinatario determinado y, reconoce que el mensaje fue recibido. RPost salvará el registro de esta transacción de forma tal que pueda posteriormente acceder a la misma e incluirla dentro, o agregarla al Recibo de Entrega RPost para dicho mensaje.

Por varias razones RPost podría no lograr alcanzar una conexión SMTP con un MTA de un destinatario o puede alcanzar dicha conexión pero no obtener el permiso para transmitir el mensaje por parte del destinatario. En ese caso, si la consulta DNS de Internet revela que la dirección de destino es servida por varios MTAs, el servidor Rpost 14 intentará entregar su mensaje a cada uno de estos. RPost seguirá intentando entregar a un MTA apropiado tan frecuentemente como los recursos del sistema lo permitan. Si después de un tiempo de duración establecida, RPost no puede entregar el mensaje a una dirección, este designará el estado para este destinatario de este mensaje como "NO-ENTREGABLE" y cesará todo intento de enviar este mensaje a la dirección de destino.

Cuando el servidor Rpost 14 es exitoso en la transmisión de un mensaje a un Servidor de destino que explícitamente soporta DSN ESMTP, RPost registrará el estado de este destinatario de mensaje como "ENTREGADO-Y-EN ESPERA-DE DSN".

Cuando el servidor Rpost 14 es exitoso en la transmisión de un mensaje al Servidor de destino a través de una conexión que no soporta explícitamente DSN ESMTP, RPost registrará el estado de este destinatario para este mensaje como "ENTREGADO".

1.3. *Post procesamiento*

Procesamiento DSN

Los DSNs de MTA serán devueltos al servidor Rpost 14 dirigidos a direcciones ficticias en su dominio propietario (por ej. "RPost.com"), esas direcciones habiendo sido construidas y descritas más arriba. El servidor Rpost 14 realizará un escaneo de todo el correo entrante dirigido al dominio y detectará los mensajes de DSN por medio de su sub-cadena (por ej. "rcpt"). Al analizar esas direcciones en la forma descrita anteriormente, el sistema puede identificar el mensaje y el destinatario que ha provocado la notificación DSN.

No hay formato estándar para los mensajes DSN; tampoco hay léxico estándar en el cual estos informen sus resultados. Para evaluar un DSN recibido, el sistema deberá buscar en la línea del asunto y en el cuerpo de los mensajes DSN palabras y frases que expresen el significado de los DSN. Por ejemplo, frases tales como "entrega exitosa" o "entregado a casilla de correo" o "fue entregado" normalmente señalan que el mensaje al cual hace referencia el DSN fue depositado en la casilla de correo del destino. Cuando el Sistema detecta frases como ésas cambiará el Estado de Entrega de este destino del mensaje a "ENTREGADO A CASILLA DE CORREO".

Frases tales como "no pudo ser entregado", "error fatal", "fracaso" y "sin éxito" típicamente señalan un DSN que reporta un fracaso por parte del MTA en entregar el mensaje al destino. Cuando el sistema detecta frases como ésas en el DSN, cambiará el registro de los Estados de Entrega del destinatario a "FRACASO".

Aunque el sistema siempre entrega el correo a un MTA propietario para el dominio de destino, esos MTAs en ocasiones reenviarán el mensaje a un servidor distinto (como podría ser el caso, por ejemplo, si el MTA receptor envía el correo desde atrás de un *firewall*). En este caso el DSN contendrá frases tales como "reenviado" o "reenviado a". En dichos casos, el sistema cambiará el Estado de Entrega a "REENVIADO".

Habiendo evaluado el DSN y actualizado el Estado de Entrega del destinatario conformemente, el sistema almacenará el DSN y cualquier archivo adjunto que este contenga de forma tal que este(os) mensaje(s) puedan ser incluidos en y/o adjuntados a un Recibo de Entrega RPost.

Administración de Mensaje

De tanto en tanto, el sistema realizará un escaneo de cada mensaje enviado y examinará el estado de cada destino de dicho mensaje para determinar si el sistema ha completado el procesamiento de entrega a ese destino. El criterio para completar dependerá del Estado de Entrega de ese destino:

ENTREGADO: Este estado indica que una copia del mensaje para este destinatario ha sido entregada a un MTA que no soporta DSN ESMTP. Dicho MTA podrá sin embargo enviar una forma de Notificación de Estado de Entrega en el caso de que el mensaje no pueda ser entregado a la Casilla de Correo del destinatario (como puede suceder, por ejemplo, si la dirección de destino no corresponde a una cuenta válida dentro del dominio). Por consiguiente, el sistema no tratará la entrega para dicho destinatario como completada hasta que transcurra un cierto período de tiempo desde la entrega al MTA del destinatario. Este período de tiempo -típicamente dos a veinticuatro horas- representa una estimación de un tiempo máximo requerido por la mayoría de servidores para retornar una notificación de fracaso de la entrega y este puede ser ajustado si el destino especifico de dominio es remoto o conocido por su lentitud a la hora de producir dichas notificaciones.

REENVIADO: este estado significa que un DSN ha sido recibido indicando que el MTA de destinatario ha dirigido el mensaje a otro MTA que no soporta DSN de ESMTP. En este caso, es sin embargo posible que el MTA al cual el mensaje ha sido entregado envíe una notificación de fracaso en la entrega en los tiempos requeridos. Como corresponde, los destinatarios con este estado son tratados como completados bajo las mismas condiciones que los destinatarios con el estado ENTREGADO.

ENTREGADO-Y-EN-ESPERA-DE-DSN: este estado indica que el MTA del destinatario soporta el DSN de ESMTP y que un DSN ha sido solicitado pero no ha sido aún recibido. Podría suceder algunas veces que aunque un MTA se identifica como soportando este servicio no proporcione sin embargo DSNs aun ante casos de entrega exitosa. Por consiguiente, el sistema observará las entregas a un destino con este estado como completado aun si no se recibe un DSN después de un intervalo de tiempo. Este intervalo -típicamente de seis a veinticuatro horas- representa una estimación del tiempo máximo típicamente requerido para que un MTA compatible devuelva un DSN.

ENTREGADO-A-CASILLA-DE-CORREO: este estado indica que un DSN señalando una entrega exitosa ha sido recibido para este destinatario y por lo tanto la entrega del mensaje a este destino ha sido completada.

FRACASO, NO-ENTREGABLE: las entregas a destinatarios con este estado son siempre tratadas como completadas.

Cuando el sistema comprueba que una entrega a todos los destinatarios de un mensaje ha sido completada, éste construirá un Recibo de Entrega para el mensaje.

Creación de Recibos de Entrega

Los Recibos de Entrega son correos electrónicos enviados al remitente original del mensaje hecho-de-registro. El recibo 20 puede contener:

1. un identificador para propósitos administrativos. Este identificador puede ser o puede incluir referencias a la identidad (*ID*) del remitente y/o el valor de la identidad Internet del Mensaje (*Internet Message-ID*) del remitente como fue recibido por el sistema;

2. la fecha y la hora en la cual el recibo fue generado;

3. el cuerpo referido del mensaje original junto con las direcciones de correo electrónico de los destinatarios pretendidos;

4. la fecha y la hora a la cual el servidor RPost recibió el mensaje;

5. una plantilla para cada destino enumerando:

   (i) la hora a la cual el MTA del destinatario recibió el mensaje y/o la hora a la cual el sistema recibió un informe DSN del MTA del destinatario;

   (ii) un Estado de Entrega del mensaje para ese destino. El Estado de Entrega referido en un Recibo de Entrega está basado en los registros internos del sistema de Estado de Entrega del destino. Estos pueden ser transcritos de la siguiente forma:

   - Entregas a destinatarios cuyo estado es FRACASO o NO-ENTREGABLE serán registradas en el recibo como “fracaso”.

   - Entregas a destinatarios cuyo estado es ENTREGADO o ENTREGADO-Y-EN-ESPERA-DE-DSN serán registradas en el recibo como “entregado a servidor de correo”.

   - Entregas a destinatarios cuyo estado es ENTREGADO-A-CASILLA-DE-CORREO serán registradas en el recibo como “entregado a casilla de correo”.

   El propósito de esos informes es advertir al lector con precisión sobre la forma de verificación de entrega que el sistema ha sido capaz de alcanzar.

6. una lista de los archivos adjuntos originales del correo electrónico junto con los digestos de mensaje por separado de cada uno de esos archivos adjuntos;

7. copias de los archivos adjuntos al mensaje original, cada archivo adjunto original siendo adjuntado al recibo;

8. transcripciones, sumarios o abstracciones de las transcripciones de todos los diálogos SMTP involucrados en la entrega del mensaje a cada destino;

9. citaciones de los cuerpos y archivos adjuntos de todos los informes DSN recibidos, incluyendo cualquier detalle sobro la entrega o la disposición del mensaje que los mismos puedan revelar; y

10. todos los archivos que fueron devueltos al sistema como archivos adjuntos a los informes DSN.

Cada uno de estos elementos del recibo pueden contar con sus propios digestos de mensaje o firmas digitales incluidas dentro del recibo. Adicionalmente, el recibo puede incluir un digesto de mensaje general cifrado único o firma digital computada y agregada como parte del recibo, proporcionando por lo tanto un código único de autentificación de mensaje que podría ser utilizado para autenticar la totalidad de la información contenida dentro del recibo. Puesto que el recibo mismo y los diálogos SMTP y los informes DSN dentro del recibo contienen estampillas de tiempo, el recibo incluye un registro no-falsificable de el/los destinatario(s) del mensaje, del contenido del mensaje y de la(s) hora(s) y ruta(s) de entrega.

Procesamiento de Notificación MUA

Las notificaciones MUA pueden ser obtenidas e incorporadas dentro de los recibos de Entrega RPost de la misma forma que los DSNs de MTA. Sin embargo, las notificaciones MTA son típicamente emitidas por MTAs receptores dentro de un rango de algunas horas de la entrega, mientras que las Notificaciones MUA no serán generadas, si es que lo son, hasta que el destinatario abra su cliente de correo electrónico MUA y lleve a cabo alguna acción con respecto al correo recibido. Por esta razón, en esta personificación de la invención, las notificaciones MUA son recolectadas separadamente de las notificaciones MTA y reportadas en "Recibos de Lectura RPost" ("*RPost Reading Receipts*") separadamente de los "Recibos de Entrega RPost" ("*RPost Delivery Receipts*").

Las notificaciones MUA obtenidas por encabezados de mensaje construidos de la forma descrita anteriormente serán devueltas a una dirección común RPost (por ej. "readreceipts@RPost.com") y cada notificación contendrá - en el campo "nombre" de su dirección - la dirección del remitente original de este mensaje. Por ser esta la única información requerida para generar un recibo de lectura RPost de la forma descrita a continuación, el sistema puede tratar con notificaciones MUA en el momento que lleguen esas notificaciones y sin necesidad de haber almacenado información alguna en sus bancos de datos con respecto al mensaje original.

Los avisos MUA pueden informar, entre otras cosas, que un mensaje ha sido leído por un destinatario, que un mensaje ha sido desplegado en la terminal del destinatario (que haya sido leído o no), que un mensaje ha sido borrado sin haber sido abierto. No hay ningún estándar regido por protocolo para el contenido o formato de los mensajes MUA. El sistema puede ser configurado de forma tal que examine el texto de los MUAs para interpretar esos informes de la misma forma que el sistema utiliza los DSNs de MTA. Sin embargo, en la presente personificación de la invención, los MUAs no son evaluados o interpretados per-el servifior Rpost 14 pero son, en cambio, reenviados al remitente para su propia evaluación de forma tal que puedan ser autenticados por RPost. Para lograr esto, el sistema creará un mensaje de correo electrónico estilado como una "Notificación de Lectura RPost", que puede incluir, entre otros items:

1. la línea de asunto de la notificación MUA recibida;

2. el cuerpo de la notificación MUA recibida citada como el cuerpo de la Notificación de Lectura;

3. la notificación MUA recibida incluida como un archivo adjunto;

4. cualquier archivo(s) adjunto(s) de la notificación MUA recibida incluidos como archivo(s) adjunto(s).

5. digestos de mensaje de la notificación MUA recibida y cualquier archivo adjunto de esa notificación;

6. una sello de fecha y hora;

7. un hash cifrado de, por los menos, los items 5 y 6 proporcionando una firma digital con sello de tiempo que pueda ser autenticada para el documento y la totalidad de sus contenidos.

Disposición del Recibo

En el caso de la presente personificación de la invención, tanto los recibos de entrega como los recibos de lectura RPost son enviados al remitente original del mensaje hecho-de-registro. Puesto que esos recibos están digitalmente firmados con un hash cifrado, RPost puede autenticar la información contenida en esos mensajes en cualquier momento que sean presentados a RPost para dicho propósito, de la manera descrita a continuación. Esto significa que una vez que este ha transmitido una copia del recibo a su remitente (con instrucciones para el remitente de conservar el recibo para sus registros), RPost no tiene necesidad alguna de retener ningún dato referente al mensaje o a su entrega y puede expurgar la totalidad de dichos registros de su sistema. Por lo tanto, RPost no necesita conservar copia alguna del mensaje original o del recibo. Esta economía de memoria de archivo le proporciona a la presente invención una ventaja sobre varios sistemas de autenticación de mensaje de conocimiento previos que requieren grandes cantidades de almacenamiento de datos por parte del proveedor de servicio.

En este caso la carga de retener datos de recibos recae en el remitente original del mensaje. Alternativamente o adicionalmente, el verificador RPost en su calidad de tercero puede, tal vez por una suma adicional, archivar una copia permanente del recibo o de algún o todos los datos del recibo. El recibo o parte(s) del mismo puede ser almacenado en cualquier dispositivo de almacenamiento de archivo apropiado, incluyendo una cinta magnética, un CD ROM u otros tipos de dispositivos de almacenamiento. Adicionalmente o alternativamente, RPost puede devolver recibos o partes del mismo a un sistema de almacenamiento dedicado este propósito que pueda ser controlado por el remitente o por la organización del remitente.

Como descrito más arriba, el recibo de información RPost incluye todos los datos del mensaje original del remitente y sus archivos adjuntos. Existen circunstancias en la cuales los usuarios del sistema podrían no querer asumir la carga de retener recibos en sus registros (por ej., por temor a la pérdida accidental de datos) pero pueden igualmente no desear que los contenidos de su mensaje queden en manos de un tercero como RPost. Conformemente, RPost puede descartar los contenidos de los mensajes pero conservar en su base de datos únicamente información que (por ej. remitente, fecha de redacción, digestos de mensaje, destinos y Estados de Entrega) pueda ser proporcionada por RPost para autenticar y verificar la entrega de un mensaje cuando le sea presentada una copia del mensaje retenido por el remitente.

Verificación

En caso de que el emisor de un mensaje requiera ulteriormente evidencia de que el correo electrónico fue enviado, entregado y/o leído, el emisor presenta el/los recibo(s) del/de los mensaje(s) a los operadores del sistema.

Por ejemplo, para poder probar que un mensaje particular fue enviado del remitente 10 al destinatario 18, el remitente 10 envía a RPost una copia del recibo 20 con una solicitud de verificación de la información contenida dentro del recibo a una casilla de correo predefinida en RPost, por ej. verify@RPost.com. RPost determina entonces si el recibo es o no es un recibo válido.

Un recibo es un recibo válido si la firma digital concuerda con el resto del recibo y si los digestos de mensaje concuerdan con las partes respectivas correspondientes del mensaje original. Específicamente, RPost realiza la función de hash sobre varias porciones del mensaje, incluyendo el cuerpo del mensaje, los archivos adjuntos y el mensaje en general, incluyendo el diálogo SMTP y los informes DSN, para producir uno o más digestos de mensaje correspondientes a la aparente copia del mensaje. RPost compara los digestos de mensaje en la aparente copia, incluyendo el digesto de mensaje en su totalidad, con el digesto de mensaje que RPost ha computado de la aparente copia del mensaje. El digesto del mensaje general puede ser comparado o bien descifrando la totalidad del digesto del mensaje recibido como la firma digital en el aparente recibo o bien cifrando la totalidad del digesto del mensaje que ha sido calculado desde la aparente copia del mensaje. Si los digestos de mensaje, incluyendo la firma digital, concuerdan, entonces el recibo es un recibo auténtico generado por RPost. Suponiendo que se utilizó una buena función de hash y que las llaves utilizadas en la función de hash criptográfica y el algoritmo de cifrado de la firma digital no han sido divulgados a otros, es virtualmente imposible que el recibo haya sido "falsificado" por la persona que presenta el recibo. Es decir, el recibo debe haber sido un recibo generado por RPost y, por lo tanto, el mensaje contenido en el recibo, la información sobre a/de (*to/from*), la fecha y la hora de entrega, el hecho de entrega exitosa, la ruta por la cual transitó el menaje y cualquier información DSN contenida dentro del recibo, debe ser una copia verdadera de la información y es exacta. RPost puede entonces proporcionar autentificación, verificación y confirmación de la información contenida dentro del recibo. Esta confirmación puede tomar la forma de un correo electrónico de confirmación, un testimonio de declaración jurada de empleados de RPost familiarizados con los métodos utilizados por RPost, testimonios en vivo declarados bajo juramento en deposiciones y en un tribunal de justicia así como otras formas de testimonio. RPost puede cobrar al remitente 10, al destinatario 18 o a cualquier otra entidad, tarifas por los diversos y respectivos servicios de confirmación. RPost puede igualmente proporcionar testimonio u otra confirmación con respecto a la no-autenticidad de un aparente recibo. Puede aportar testimonio en conformidad con las Reglas Federales de Evidencia (*Federal Rules of Evidence*) 901(9), 901 (10), 803(6), 803(7), 1001-1004, 1006, 702-706, las reglas estatales de evidencia correspondientes y otras reglas aplicables.

En resumen, el sistema proporciona evidencia confiable basada en el testimonio de un tercero desinteresado que un mensaje particular que cuenta con un contenido particular fue enviado, cuando fue enviado, quien lo envió, quien lo recibió, cuando fue abierto para su lectura y cuando fue borrado. Esta evidencia puede ser presentada en cualquier momento que surja una disputa en relación al contenido y a la entrega de mensajes, como por ejemplo en la formación de contratos, en el momento de la compra de acciones u órdenes de venta y en muchas otras aplicaciones. Los operadores del sistema puedan atestiguar sobre la precisión de la información contenida en el recibo mismo sin necesidad de que los operadores conserven registro alguno o copia alguna de la información contenida en el recibo.

Una ventaja significativa del sistema es que puede ser utilizado por MUAs existentes sin necesidad de realizar cambio alguno en el mismo. Debido a que la computación, el cifrado, la interrogación y el diálogo ESMTP, la recolección de informes DSN y la compilación de recibo, son realizadas por un tercero, el servidor Rpost 14, ninguna de estas funciones necesita ser implementada dentro de algún equipo del usuario. Por consiguiente, los usuarios pueden sacar ventaja del sistema rápida y fácilmente.

En la personificación de la invención descrita anteriormente, el servidor Rpost 14 hace de registro la entrega de todos los mensajes que pasan a través del mismo. Como alternativa, un servidor Rpost 14 puede hacer de registro úni-

camente aquellos mensajes que cuentan con ciertos destinos (por ej. externos a una organización) o que son enviados desde ciertos remitentes (por ej. un grupo de relaciones de clientela). Sino, o adicionalmente, el servidor Rpost 14 puede hacer de registro únicamente aquellos mensajes que contienen caracteres distintivos o cadenas en el asunto o cuerpo del mensaje. Por ejemplo, el servidor puede hacer de registro únicamente mensajes en lo cuales el remitente haya incluido "Hacer de Registro" ("*Make of Record*") o "(*MR*)" en el asunto del mensaje. La totalidad de otros mensajes podrá ser entregada por el servidor Rpost 14 o algún otro servidor que funcione como un MTA convencional de Internet.

En esta personificación, RPost puede obtener ingresos en una variedad de formas. Por ejemplo: RPost puede cobrarle a un remitente 10 de menaje o a su organización una suma basada en cada- mensaje, en la cantidad de kilobytes, en base a una suma básica periódica tal como mensual o en una combinación de todas o cualesquiera de las anteriores. RPost puede también cobrar tarifas por la autentificación y la verificación de un recibo, con una lista de tarifas dependiendo de si la verificación solicitada es un simple correo electrónico de retorno, una declaración escrita o jurada, una declaración jurada por escrito en deposición o en estrados judiciales, o un testimonio jurado de experto en deposición o tribunal de justicia. Si los usuarios optan por que RPost conserve copias de esos recibos, RPost podrá cobrar tarifas de almacenamiento por artículo y por kilobyte/mes.

Diagrama de flujo para hacer de registro un mensaje saliente

Las Figs. 2A-2G constituyen un gráfico de flujo mostrando una operación ejemplar de la primera personificación del sistema. Modificar este gráfico de flujo para aplicarlo a otras personificaciones está al alcance de cualquier persona familiarizada con software en general y los protocolos del correo electrónico.

La Fig 3A, Pre-procesamiento, enseña los pasos a seguir con un mensaje antes de que sea transmitido por el Servidor de Hacer de Registro (el Sistema).

Para hacer de registro un mensaje de correo electrónico, en el paso 201 un emisor/remitente/usuario crea un mensaje de correo electrónico utilizando cualquier Agente de Usuario de Correo (MUA) de Internet. Posibles MUAs incluyen: (1) programas de correo electrónico del lado del cliente; (2) programas de correo electrónico basados en el servidor 45; (3) servicios de correo electrónico basados en la Web; y (4) formularios HTML consignados a través de páginas web. El mensaje puede contener archivos adjuntos según se describe en las Solicitudes para Comentarios (*Requests for Comments*) (RFC5) 822, 2046 y 2047, las cuales están incorporadas en la presenta a título de referencia. Las RFCs son una serie de notas sobre Internet que exponen los múltiples aspectos de la comunicación por computadora, concentrándose en protocolos, procedimientos, programas y conceptos de conexiones de red.

En esta personificación, el sistema funciona como el servidor de correo saliente del remitente y por lo tanto el mensaje del remitente será directamente transferido al servidor RPost por el MUA del remitente (paso 202).

En el paso 203, el sistema crea una copia del mensaje original para ser almacenado para un procesamiento ulterior.

En el paso 204, el sistema crea un registro en una base de datos que puede incluir información tal como: la hora a la cual el mensaje fue recibido por el servidor, los nombres y tamaños) de los archivo(s) adjuntos(s) del Mensaje, el nombre (si es conocido) de cada destino del mensaje; la dirección Internet de cada destino; la hora a la cual el mensaje fue entregado al MTA de destino (inicialmente este valor es nulo) y una unidad que registra el Estado de Entrega de cada destino.

En el paso 205, el Estado de Entrega de cada destino esta establecido en "NO-ENVIADO".

En el paso 206, el sistema genera y archiva un digesto de mensaje o huella digital generada a partir del cuerpo del mensaje.

En el paso 207, el sistema genera y almacena un hash o digesto de mensaje para cada archivo adjunto incluido en el mensaje.

En el paso 208, el sistema puede crear una copia modificada del mensaje original. En esta segunda copia (paso 209), la linea de asunto original del mensaje puede ser modificada para indicar que esta copia ha sido hecha de registro (por ej. incluyendo la mención "Hecho de Registro").

En el paso 210, puede añadirse al cuerpo del mensaje una notificación que el mensaje ha sido hecho de registro por el sistema junto con vínculos al sitio Web de la red de Internet (Word Wide Web site).

En el paso 211, pueden agregarse encabezados de correo electrónico solicitando una notificación de lectura en una variedad de formatos de encabezamiento reconocidos por varios MUAs. Las solicitudes de notificación dirigen la notificación de retorno a una dirección asociada con el sistema: por ejemplo, "readreceipts@RPost.com". Dichos encabezados también incluirán la dirección del remitente original del mensaje en el campo "nombre" de la dirección a la cual la notificación del MUA debe ser enviada.

Habiendo completado el Pre-procesamiento, el sistema ahora transmitirá una copia del mensaje a cada uno de los destinos, como ilustrado en la Fig. 2B.

La Fig 2B ilustra los pasos provistos para transmitir un mensaje hecho de registro. Como el paso 220 indica, el proceso proporciona una transmisión separada para cada destinatario del mensaje.

En el paso 221, el sistema cambia el campo del encabezado de su copia de trabajo del mensaje para mostrar el mensaje como proviniendo "DE:" ("*FROM:*") un remitente cuyo nombre es el remitente original del mensaje pero cuya dirección es una dirección "RPost.com" construida con:

a) una cadena utilizada para identificar notificaciones MTA que retornan (por ej. "RCPT");

b) una cadena que identifica como único el mensaje que está siendo enviado;

c) una etiqueta que identifica como único el destino al cual esta copia está siendo enviada.

En el paso 222, utilizando el nombre de dominio del destino al cual se está enviando en ese momento, el sistema ejecuta una consulta de intercambio de Servidor de Nombre de Dominio para encontrar la dirección del o los MTA(s) responsable(s) de recolectar correo para direcciones en este dominio.

En el paso 223, el sistema intenta realizar una conexión de telnet directa con el MTA del destino. Si la conexión falla, el sistema intentará realizar nuevamente la conexión. Siempre que el sistema no haya excedido un número máximo de re-intentos (227) para este destino, el sistema entonces intentará realizar la conexión, tal vez utilizando otro servidor MX para el dominio de destino (228).

Si, tras realizar un número máximo de re-intentos, el sistema no logra conectar con un MTA para ese destino, el sistema, como se detalla en el paso 226, registrará este Estado de Entrega de destino como "NO-ENTREGABLE" y cesará de intentar entregar este mensaje a su destino.

Al conectarse con el MTA de destino, el sistema iniciará a hacer de registro sus diálogos de (E)SMTP con el MTA (225).

En el paso 229, el sistema intentará iniciar un intercambio SMTP Extendido (ESMTP) con el MTA de destino al emitir un comando "EHLO".

Si el MTS de destino soporta el ESMTP, el sistema determinará entonces (230) si el MTA de destino soporta la función de SMTP VERIFICAR (*VERIFY*). Si el MTA soporta VERIFICAR, el sistema intentará entonces determinar si la dirección de destino es una dirección válida dentro del dominio (231).

Si la dirección no es válida, entonces, como en el paso 232, el sistema registrará el Estado de Entrega de este destino como "FRACASO" y cesará los intentos de entrega de este mensaje al destino.

Si la dirección es válida o si el servidor de ESMTP no soporta "VERIFICAR", el sistema determinará entonces (233) si el MTA que recibe soporta el servicio DSN de Notificación de Estado de Entrega ESMTP.

Si el MTA no soporta el DSN ESMTP, el sistema transmitirá el mensaje con solicitudes ESMTP para notificar al remitente nominal del éxito o del fracaso de la entrega del mensaje (234). Habiendo transmitido el mensaje, el sistema registrará el Estado de Entrega de este destino como "ENTREGADO-Y-EN-ESPERA-DE-DSN" (235).

Si el MTA que recibe no soporta el SMTP Extendido, el sistema transmitirá el mensaje utilizando el SMTP (236) y registrará el estado de los destinos como "ENTREGADO" (237).

Habiendo entregado el mensaje, el sistema almacenará entonces el diálogo (E)SMTP, registrando la entrega de modo que este pueda ser recuperado ulteriormente (238) e intentar enviar el mensaje a otro destino.

Habiendo transmitido un mensaje a su(s) destino(s), el sistema debe realizar múltiples funciones para poder obtener información sobre la disposición del mensaje. La Fig. 2C ilustra el proceso por medio del cual el sistema procesa Notificaciones MTA devueltas por MTAs del destinatario.

Por razón del formato utilizado en el encabezado de mensajes enviados ilustrado en la Fig 2B paso 221, las notificaciones de mensaje MTA serán entregadas a direcciones locales ficticias en el servidor. El sistema será capaz de detectar estas notificaciones por una cadena (por ej. "rcpt") alojada en sus direcciones (241). Al analizar la dirección, según se ilustra en 242, el sistema puede determinar cual mensaje provocó la notificación de recibo en cual destino.

En el paso 243, el sistema realiza. un escaneo de la linea de asunto y del cuerpo de los MTAs recibidos en búsqueda de frases que indican que el MTA está informando una entrega exitosa, una entrega fallida, o que el mensaje ha sido reenviado a otro servidor.

En el caso de que el proceso en paso 243 revele que la notificación está informando una entrega exitosa, el sistema, como se ilustra en el paso 245, cambiará el Estado de Entrega del destino relevante del mensaje relevante a "ENTREGADO-A-CASILLA-DE-CORREO".

Si el sistema determina que la notificación MTA está informando un fracaso de la entrega, el sistema (247) cambiará el Estado de Entrega del destino relevante del mensaje relevante a "FRACASO".

En el caso de que el sistema determine que la notificación MTA indica que el mensaje fue reenviado a otro servidor, el sistema, como se ilustra en el paso 249, cambiará el Estado de Entrega del destino relevante del mensaje relevante a "REENVIADO".

Habiendo procesado la Notificación MTA, el sistema salvará este mensaje y todos sus archivos adjuntos de manera tal que puedan ser obtenidos y utilizados en la construcción de un recibo para este destino (250).

De tanto en tanto, como se ilustra en la Fig. 2D, el sistema examinará el estado de cada mensaje para determinar si el sistema ha recuperado todas las notificaciones MTA que debería recibir para cada destino de mensaje y podrá entonces proceder a construir el recibo para el mensaje.

El sistema examinará el Estado de Entrega de cada destino del mensaje.

Si algún destino tiene el Estado de Entrega "NO-ENVIADO", entonces el procesamiento del mensaje no está completado. (252).

Si el Estado de Entrega de un destino es "ENTREGADO-Y-EN-ESPERA-DE-DSN", entonces el sistema no observará el procesamiento de este destino como completado a menos que, como se ilustra en el paso 254, el tiempo desde la entrega del mensaje haya excedido el periodo de espera del sistema (por ej. 24 hrs.).

Si el Estado de Entrega de un destino es "ENTREGADO" (257), entonces el sistema observará el procesamiento de este destino como completado siempre que (258) haya transcurrido un período de tiempo que los operadores del sistema consideren como suficiente para haber recibido una notificación del fracaso de la entrega de los MTAs de destino. (Por ej. 2 horas).

Cualquier otro Estado de Entrega de destino (por ej. "FRACASO", "NO-ENTREGABLE", "ENTREGADO-A CASILLA-DE-CORREO" es considerado como un procesamiento completado.

Si el procesamiento de cualquiera de los destinos del mensaje no es completado, el sistema no realiza otra acción sino que procede a considerar otros mensajes en el sistema (paso 255).

Sin embargo, como se ilustra en el paso 259, si el procesamiento de cada destino del mensaje es completada, el sistema generará un Recibo de Entrega para el mensaje.

Según se ilustra a nodo de ejemplo en la Fig. 2E, el recibo puede incluir:

Un identificador para propósitos administrativos como en el bloque 271. Este identificador puede ser, o puede incluir, una referencia a la identidad del remitente y/o el valor de la identidad Internet del mensaje (*Internet Message-ID*) del remitente como se recibió por parte del sistema.

Como en el bloque 272, pueden también incluirse el cuerpo referenciado del mensaje original 12 junto a las direcciones de los destinatarios pretendidos del correo electrónico.

Como en el bloque 273, una plantilla para cada destinatario enumerando:

a) la hora a la cual el MTA del destinatario recibió el mensaje y/ola hora a la cual el sistema recibió el DSN del MTA del destinatario;

b) el informe de Estado de Entrega del mensaje para ese destino, por ej., "Entregado a Servidor de Correo", "Entregado a Casilla de Correo", "Reenviado", "Fracaso en la Entrega", o "No-Entregable".

Como en el bloque 274, una lista de los archivos adjuntos originales del correo electrónico junto con sus valores de hash o digestos de mensaje individuales.

Como en el bloque 275, las transcripciones o abstracciones de las transcripciones de todos los diálogos SMTP involucrados en la entrega del mensaje para cada destino.

Como en el bloque 276, citas de los cuerpos y de los archivos adjuntos de todos los DSNs recibidos, incluyendo cualquier detalle de la entrega o de la disposición del mensaje que estos puedan revelar.

Como en el bloque 277, el sistema puede adjuntar al recibo copias de todos los archivos adjuntos del mensaje original y, como en el bloque 278, el sistema puede adicionalmente adjuntar archivos devueltos al sistema como archivos adjuntos a los DSNs.

En el paso 279, habiendo generado el texto del recibo hasta ahora, el sistema genera entonces un primer hash para el mensaje de correo electrónico y un segundo hash para cualquier archivo adjunto al cuerpo del recibo y calcula una firma digital para cada uno de los hash utilizando una llave de cifrado conocida únicamente por los operadores del sistema. El cifrado puede emplear, por ejemplo, el Estándar para Cifrado de Datos (*Data Encryption Standard*) descrito en la Publicación para Estándar de Procesamiento de Información Federal (*Federal Information Processing Standard Publication*) 4-2 (FIPS PUB 46-2), el Estándar de Cifrado de Datos (*Data Encryption Standard*), del Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*), incorporados en la presente a título de referencia. Alternativamente, pueden utilizarse otros conocidos o nuevos métodos de cifrado del valor hash.

En el paso 280, el hash cifrado es entonces agregado al final del mensaje como la "firma digital del documento".

En el pago 281, el recibo 20, ahora completo, puede ser enviado por correo electrónico al remitente con el consejo de que sea conservado para los registres del remitente. En el paso 282, el sistema puede ahora borrar todas las copias del mensaje original, los archivos adjuntos y los DSNs. Alternativamente, en lugar de enviar el recibo al remitente, el sistema puede almacenar el recibo o ambos, tanto el remitente como el sistema, pueden archivar el recibo.

Porque las notificaciones MUA son devueltas únicamente bajo opción del destinatario y únicamente cuando el destinatario realice alguna acción con respecto al mensaje recibido, las personificaciones del sistema pueden escoger tratar esos mensajes devueltos diferentemente de las notificaciones MTA.

La Fig. 2F ilustra como esas notificaciones MUA pueden ser tratadas por el sistema. Las notificaciones MUA son solicitadas por el sistema al incluir varios encabezados en mensajes salientes de la manera mostrada en la Fig 2A, paso 211. Esos encabezados dirigen MUAs compatibles para que envíen notificaciones a una dirección de sistema (por ej. "readreceipts@Rpost.com") creada para este propósito. Los encabezados también utilizan, en el campo 'nombre' de esta dirección de retorno, la dirección de correo electrónico del remitente original del mensaje. Por consiguiente, en el paso 286, cuando las notificaciones MUA son devueltas a readreceipts@RPost.com el sistema puede, al examinar la dirección de la notificación, determinar la dirección a la cual la notificación de lectura debe ser enviada.

Cuando llega el recibo de lectura desde un MUA de destino, el sistema, en el paso 287, genera un recibo de lectura que contiene el asunto de la notificación MUA recibida como su asunto e incorpora, en su cuerpo de mensaje, el cuerpo de la Notificación MUA recibida.

En el paso 288, el sistema adjunta al recibo cualquier archivo que pueda acompañar al recibo MUA (típicamente, esos pueden incluir detalles de la entrega o de la disposición así como referencias de identificación al correo electrónico original).

En el paso 289, el sistema genera un hash para cualquier archivo adjuntado al recibo y registra este hash en el cuerpo del recibo.

En el paso 290, el sistema genera un hash para el cuerpo del recibo y sus archivos adjuntos, cifra este hash y agrega el resultado al mensaje como "firma digital del documento".

En el paso 291, el sistema envía el recibo resultante al remitente del mensaje. En el paso 292, habiendo enviado este recibo, el sistema puede borrar todos los registros internos de la transacción.

III. *RPOST como personificación de servidor de correo secundario*

La Fig. 3 es un diagrama de sistema de una segunda personificación de la presente invención en la cual el servidor Rpost 14 no funciona como el MTA primario del usuario sino que trabaja en colaboración con otro MTA. En esta personificación, el remitente puede elegir hacer de registro un mensaje saliente en particular al incluir algún tipo de etiqueta en un mensaje saliente, en el asunto del mensaje, o en las direcciones del mensaje. Por ejemplo, si y solo si un remitente incluye el símbolo "(Hecho de Registro)" "(*Made of Record*)" o '(MR)' en el asunto del mensaje del MTA del remitente dirigirá el mensaje para que sea transmitido a través del servidor Rpost 14 para generar un recibo.

En esta personificación, los operadores de RPost reciben ingresos del operador del MTA del remitente a razón de mensaje y/o de cantidad de kilobyte transmitido.

IV. *Personificación de CC a RPOST*

La Fig. 4 es un diagrama de sistema de una tercera personificación en la cual una copia carbón ("cc") es enviada al servidor Rpost 14. En esta personificación, el usuario o remitente 10 del mensaje puede utilizar un MUA y un MTA estándar sin modificación. El remitente 10 del mensaje redacta el correo electrónico teniendo un cuerpo de mensaje y cualquier número de archivos adjuntos y lo dirige para enviar al destinatario 18, junto con cualquier copia carbón (cc) y copia carbón invisible (cci) que desee. Adicionalmente, el remitente 10 del mensaje agrega una dirección de cc con

destino RPost. El servidor Rpost 14 etiqueta el mensaje como anteriormente y envía el mensaje etiquetado incluyendo archivos adjuntos al MTA 16 del destinatario y a cualquier cc designado. Con el recibo de dicha copia, el servidor Rpost 14 puede enviar un correo electrónico confirmando recibo de dicha copia.

El destinatario 18 y otros destinatarios del mensaje recibirán ahora dos versiones del mismo mensaje: una primera versión del mensaje recibido directamente del remitente 10 y una segunda y etiquetada versión que ha sido dirigida desde RPost. Una vez que RPost recibe confirmación del MTA 16 del destinatario que la versión etiquetada del mensaje fue satisfactoriamente recibida por el MTA 16 del destinatario, el servidor Rpost 14 redacta un mensaje de recibo 20 como anteriormente y envía el recibo al remitente 10 para sus registros.

Pueden generarse ingresos al establecer cuentas para dominios emisores de mensajes o para remitentes de mensajes individuales y cobrando a las cuentas de usuario por uso, por kilobyte, por mes o una combinación de estos. Pueden igualmente generarse ingresos colocando anuncios en los recibos y por los servicios de autentificación y verificación previamente descritos.

V. *Personificación de sitio Web*

La Fig. 5 es un diagrama de sistema de una cuarta personificación. En esta personificación, el servidor 14 RPost está asociado con un sitio Web en el cual un usuario redacta mensajes. El remitente 10 del mensaje visita el sitio Web de RPost y redacta su mensaje en el sitio Web completando la información de destinatarios deseados “A”, “cc”, “ccl”, “Asunto” y el texto del mensaje. Los archivos adjuntos pueden ser agregados utilizando características disponibles en buscadores y servidores Web. En estas persónifcación, el remitente proporciona además una dirección a la cual el recibo hecho-de-registro puede ser enviado. El servidor Rpost 14 envía el recibo al remitente 10 a través del MTA del remitente.

Pueden generarse ingresos al establecer cuentas para dominios emisores de mensajes o para los remitentes individuales de mensajes y cobrando a las cuentas de los usuarios por mensaje, por kilobyte, por mes, o una combinación de los mismos. Pueden igualmente generarse ingresos colocando anuncios en los recibos y por los servicios de autentificación y verificación, como descrito previamente.

VI. *Personificación de MUA basado en la Web*

La Fig. 6 es un diagrama de sistema de una quinta personificación. En esta personificación, el servidor Rpost 14 esta asociado a un Agente de Usuario de Correo basado en la Web. Además de permitirle a los usuarios redactar correo a través de un buscador Web, dicho MUA le proporciona a los abonados casillas de correo visibles que despliegan mensajes archivados en el sitio de servidor Web. Los abonados a dicho servicio obtienen acceso a cuentas de correo mediante el uso de nombres de usuario y contraseñas. En esta personificación, el remitente 10 del mensaje visita el sitio Web de RPost, accede a una cuenta de correo electrónico al ingresar su nombre de usuario y su contraseña y redacta su mensaje, que puede ser transportado para una entrega al servidor Rpost 14. Los recibos generados por el servidor Rpost 14 son devueltos a una casilla de correo situada en la Web asociada con la cuenta del abonado.

Además de las fuentes de ingresos disponibles en otras personificaciones, en esta personificación los operadores pueden cobrar sumas a razón de archivo de recibos conservados en la casilla de correo situada en la Web.

En todas esas personificaciones, el recibo puede servir como evidencia que:

(1) el emisor envió un mensaje de correo electrónico;

(2) el mensaje fue enviado a cierta hora;

(3) el correo electrónico fue dirigido a ciertos destinatarios;

(4) el correo electrónico fue entregado a la casilla de correo de cada uno de los destinatarios pretendidos;

(5) el correo electrónico fue entregado en una hora determinada;

(6) el correo electrónico fue entregado por cierta ruta de red; y

(7) el mensaje de correo electrónico y sus archivos adjuntos tenían el contenido especifico registrado en el recibo.

Asimismo, el sistema bajo ciertas circunstancias genera un recibo separado que puede ser utilizado como evidencia que:

(1) el correo electrónico fue examinado a través del Agente de Usuario de Correo (MUA) del destinatario; y

(2) el destinatario realizó ciertas acciones en respuesta al mensaje, por ej., lectura o eliminación del correo electrónico, en un momento particular.

Como con las otras personificaciones, esta personificación produce evidencia documentada que puede ser avalada y verificada por operadores terceros desinteresados del sistema en referencia a la entrega y la integridad de un mensaje electrónico. En otras palabras, el sistema puede ser concebido como un transformador del correo electrónico para hacer correo electrónico de registro que pueda ser utilizado posteriormente para demostrar que un mensaje de correo electrónico en particular fue enviado, que fue satisfactoriamente entregado, cuando y como.

Si una disputa llegase a surgir en algún momento, la disputa puede ser resuelta a través del recibo generado por el sistema por cuanto el recibo está codificado de tal manera que los operadores del sistema pueden determinar la autenticidad del recibo como el producto del sistema. Por consiguiente, los operadores del sistema pueden avalar y atestiguar la exactitud de la información contenida en un recibo auténtico, apoyándose únicamente en la información contenida en el recibo mismo y sin necesidad que los operadores preserven registro alguno o copia alguna de la información contenida en el recibo.

Además de estos beneficios, los recibos generados por el sistema pueden también ser útiles como evidencia de la existencia y la autoría de dichos materiales según sean transmitidos a través del sistema. Además, el sistema es fácil de utilizar ya que puede ser utilizado desde cualquier programa/MUA de cliente de correo de Internet, de forma tal que no se requiere software adicional alguno.

Diagrama de flujo para la validación de un recibo

La Fig. 7 es un diagrama de flujo que ilustra un método ejemplar para la validación de un recibo. En el caso de que el remitente de un mensaje requiera evidencia que un correo electrónico fue enviado y entregado (y/o leído) el remitente presenta el recibo correspondiente al mensaje a los operadores del sistema, en el paso 700. Los operadores del sistema, en el paso 702, separan y descifran entonces la firma digital del documento añadida al recibo. En el paso 703, los operadores generan un hash del resto del documento, incluyendo archivos adjuntos.

En el paso 704, si el valor actual de hash no concuerda con el valor de hash descifrado, entonces el sistema genera in informe, señalando que RPost no puede autenticar el recibo como un registro exacto de la entrega o de los contenidos del mensaje descritos en el recibo.

Si el hash descifrado es equivalente al hash actual del mensaje, el sistema puede, como en el paso 706, garantizar que la información contenida en el cuerpo del mensaje no ha cambiado desde que el recibo pasó a través del sistema. Si el mensaje original no contiene archivos adjuntos, el sistema podrá generar en ese momento un informe que garantiza que el recibo es un registro exacto de los contenidos del mensaje y su entrega por medio del servidor RPost.

Si el recibo informa que el mensaje original contenía archivos adjuntos, entonces el recibo también informa acerca del nombre y del valor de hash de cada uno de los archivos adjuntos. Al generar el recibo, todos los archivos adjuntos del mensaje original son adjuntados sin cambios al recibo. Conformemente, el sistema generará, para cada uno de dichos archivos adjuntos, un hash del archivo adjunto (708) y lo compara con el valor de hash registrado en el cuerpo del recibo (709).

Si el valor de hash calculado de un archivo coincide con el valor incluido en el recibo, el sistema puede garantizar que el archivo adjunto al recibo es idéntico a aquel adjuntado al mensaje como fue originalmente entregado. Si los valores de hash no coinciden, entonces el sistema informará que no puede garantizar que el archivo adjuntado al recibo es idéntico al archivo adjuntado al mensaje original.

Habiendo realizado este cálculo para cada archivo adjuntado al mensaje original, el sistema prepara un informe que notifica sobre la autenticidad del recibo y cada uno de los archivos adjuntos (710) o que informa acerca del fracaso de la validación (712).

Habiendo completado su evaluación, el sistema agregará entonces una copia del recibo y todos los archivos adjuntos al informe que ha generado y lo enviará por correo electrónico a la dirección de retorno del usuario que sometió el informe para su validación.

Registrar Correos Electrónicos Entrantes

La Fig. 8 es un diagrama de sistema que ilustra otra personificación de la invención, según la cual los correos electrónicos entrantes son hechos-de-registro. En esta personificación, un remitente 60 de mensaje envía un correo electrónico 70. El MTA 62 del remitente envía el mensaje 70 hacia Internet como de costumbre. Sin embargo, en esta personificación RPost contrata con el suscriptor de servicio/destinatario 68 para hacer de registro los correos electrónicos entrantes. Según el acuerdo, RPost es designado junto con Network Solutions, Inc. (NSI) u otra autoridad de nombre de dominio, como destinatario de correo (servidor MX) para el destinatario 68. Esto causa que el pedido del Servicio de Nombre de Dominio (DNS), realizado por el MTA 62 del remitente, retorne a la dirección IP de RPost como la dirección IP para el destinatario, lo que a su vez causa que el MTA 62 del remitente envíe el mensaje de correo electrónico al servidor RPost 64. El servidor RPost 64 actúa como un MTA de SMTP, POP, POP3 o IMAP (conjuntamente, "servidor cte correo POP") para el destinatario 68. Los MTAs de SMTP, POP e IMAP son gobernados por RFC 821, el protocolo de SMTP, Protocolo de Oficina Postal RFC 1939 (*Post Office Protocol*), Protocolo Versión 4 rev 1 (que hizo obsoleto RFC173O), incorporados en la presente a titulo de referencia.

El servidor RPost 64 prepara una versión 74 hacer-de-registro del mensaje original 70 y coloca esta versión 74 hecha-de-registro dentro del casillero de destinatario 68 en lugar de, o adicionalmente a, el mensaje original 70. La versión hecha-de-registro puede contar con todas las características y las opciones de verificación e información discutidas anteriormente en conexión con recibos de correo electrónico. Esta información puede incluir, sin limitase a: los digestos de mensaje individuales para cada uno del cuerpo y texto del mensaje, la información de a/de (*to/from*), otra información de encabezado, cada archivo adjunto, un digesto de mensaje general y una firma digital así como la información de ruta del mensaje y las etiquetas. La versión 74 hecha-de-registro del mensaje 70 como se muestra en Fig. 6 incluye el cuerpo del mensaje, incluyendo la información de encabezado, un archivo adjunto, los digestos de mensaje separados para cada uno y una firma digital o un digesto de mensaje cifrado. Las funciones de hash y cifrado son realizadas utilizando frases privadas o llaves privadas conocidas únicamente por los operadores del sistema. La versión 74 hecha-de-registro es puesta a disposición del destinatario 68 para su inspección o descarga a través del MUA del destinatario.

El servidor RPost 64 puede opcionalmente enviar un correo electrónico de confirmación 72 al remitente 60 del mensaje. El mensaje de confirmación 72 puede ser un simple mensaje de texto indicando que un mensaje fue recibido y hecho-de-registro. El mensaje de Confirmación 72 también puede incluir un mensaje tal como “Su mensaje de correo electrónico fue recibido el 24 de Marzo del 2000 a las 2:05 p.m. La firma digital del mensaje era [firma digital de 128-bit]. Para mayor información, visite nuestro sitio Web en www.RPost.com”. Alternativamente, o adicionalmente, el mensaje de confirmación 72 puede incluir toda la información contenida en la versión 74 hecha-de-registro.

Por lo tanto, el sistema puede proporcionar al destinatario 68 del mensaje un recibo 74 u otra confirmación demostrable que indique que:

(1) el destinatario recibió un mensaje de correo electrónico;

(2) el mensaje fue recibido a una hora determinada;

(3) el correo electrónico fue dirigido desde un determinado remitente;

(4) el mensaje aparenta haber sido entregado por una cierta ruta de red; y

(5) el mensaje de correo electrónico y sus archivos adjuntos tenían un contenido específico.

Conformemente, el sistema proporciona evidencia, que puede ser avalada por los operadores del sistema, que mensajes electrónicos y documentos particulares fueron entregados a destinatarios teniendo cierto contenido y presentándose a si mismos como habiendo provenido de ciertos remitentes.

La Fig. 9 es un gráfico de flujo ilustrando un ejemplo de hacer de registro correo entrante. En el paso 901, el servidor RPost 64 recibe un nuevo mensaje de correo electrónico. En el paso 902, el sistema genera un(a) hash/firma digital de los contenidos del mensaje incluyendo los encabezados y archivos adjuntos del mensaje. Adicionalmente, el sistema puede generar un hash separado para cada archivo adjunto del mensaje. En el paso 903, el sistema cifra el/los hash(es) utilizando una llave de cifrado conocida únicamente por los operadores del sistema. En el paso 904, el/los resultantes hash(es) cifrados son entonces agregados al cuerpo del mensaje. En ese momento, en el paso 905, el mensaje modificado puede ser puesto a disposición para su inspección o descarga a través del MUA del destinatario.

La Fig. 10 es un gráfico de flujo de un ejemplo de validación de un mensaje de correo electrónico recibido hecho-de-registro. En el paso 1000, en el caso de que el destinatario de un mensaje deba requerir evidencia que un correo electrónico con un contenido especifico fue recibido a un hora en particular, el destinatario puede presentar una copia de la versión 74 hecha-de-registro (Fig. 8) del mensaje de correo electrónico 70 a los operadores del sistema para su verificación. Para verificar el mensaje, en el paso 1001, el sistema separa y descifra la firma digital del documento agregada al mensaje. En el paso 1002, el sistema genera un hash del resto del documento y uno por cada archivo adjuntado al mensaje. En los pasos 1003 y 1004, los hash son comparados. Si el/los hash del documento coinciden con el/los hash descifrados, entonces el mensaje y sus archivos adjuntos han pasado a través del sistema y no han sido alterados desde su entrega al destinatario.

Habiendo determinado que el correo electrónico no ha sido alterado, los operadores del sistema pueden garantizar que:

(1) el correo electrónico fue recibido por el sistema en determinado momento de tiempo;

(2) el correo electrónico pretende haber arribado al sistema por una cierta ruta de Internet;

(3) el correo electrónico pretende ser de cierto remitente; y

(4) el correo electrónico y sus archivos adjuntos fueron entregados con el contenido especifico que contienen actualmente.

Por otra parte, en el paso 1006, si los valores de hash no coinciden, entonces el operador no puede garantizar que el correo electrónico es auténtico, por ej., que el correo electrónico es una versión exacta de un correo electrónico que fue recibido por el sistema.

La Fig. 11 ilustra como la invención puede ser utilizada por un negocio que utiliza herramientas electrónicas (un "negocio electrónico" o "e-business"). El e-business 30 puede utilizar el sistema para hacer-de-registro todos los mensajes de correo electrónico entrantes y salientes de sus clientes 34. En este caso, el sistema incluye el servidor 36 de Protocolo de Oficina Postal (POP) y el servidor 38 Protocolo Simple de Transferencia de Correo (SMTP). Por ejemplo, el e-business 30 puede configurar su sitio Web para que envíe formularios de correo electrónico a sus clientes y para dirigir consultas y quejas 40 de clientes 34. Las consultas, quejas, órdenes, ofertas de compra y otra información 46 hechas-de-registro son enviadas al e- business 30 por el sistema. Se proporcionan entonces recibos a los clientes 34 mediante el servidor 38 de SMPT. De esta forma, no cabe más duda sobre si el cliente envió o no la comunicación y lo que contenta. Asimismo, el e-business puede configurar un sitio Web 32 a través del servidor RPost para que cada comunicación con los clientes pueda ser hecha-de-registro. En otras palabras, a través del formulario de datos del sitio Web, las órdenes 42 y respuestas automatizadas 44 pueden ser hechas-de-registro a través del servidor del sistema; Además, cualquier confirmación, aviso de cobro, asistencia al cliente y ofertas especiales 48 enviadas por el e-business a clientes 34 pueden ser hechas-de-registro y la confirmación enviada al cliente para eliminar argumentos sobre qué fue ordenado, cuándo y por quién. Si se desea, pueden proporcionarse recibos idénticos para ambos, los clientes 34.y el e-business 30. Alternativamente, las funciones del servidor POP 36 y el servidor SMTP 38 pueden ser combinadas en un único servidor de sistema.

POP es un protocolo utilizado para recuperar correo electrónico de un servidor de correo electrónico. Múltiples aplicaciones de correo electrónico (en ocasiones llamadas clientes de correo electrónico) utilizan el protocolo POP, aunque algunas pueden utilizar el más reciente Protocolo de Acceso a Mensajes de Internet (*Internet Message Access Protocol*) (IMAP). Una versión de POP, llamada POP2, requiere que el SMTP envíe mensajes. Una versión más reciente, POP3, puede ser utilizada con o sin SMTP. SMTP es un protocolo para enviar mensajes de correo electrónico entre servidores. Varios sistemas de correo electrónico que envían correo electrónico por Internet utilizan el SMTP para enviar mensajes de un servidor a otro; los mensajes pueden en ese momento ser recuperados con un cliente de correo electrónico que utilice ya sea POP o IMAP. Adicionalmente, el SMTP es generalmente utilizado para enviar mensaje de un cliente de correo a un servidor de correo. Los servidores de Correo Electrónico pueden utilizar una variedad de protocolos para comunicarse con Internet. Los protocolos comúnmente utilizados incluyen al SMTP, POP3 e IMAP4. Los lectores de correo se encuentran al extremo opuesto del servidor. Siendo que los servidores de correo reciben mensajes vía SMTP, los lectores de correo electrónico envían correo electrónico a un servidor de correo utilizando SMPT. De igual forma, teniendo en cuenta que los servidores de correo envían mensajes utilizando POP3 y opcionalmente IMAP4, los lectores de correo reciben mensajes de servidores de correo utilizando el protocolo POP3 o IMAP4.

Aunque todo lo descrito más arriba generalmente describe un sistema y método de verificación que un correo electrónico fue enviado y/o recibido, la invención divulgada y reivindicada en solicitud 09/626,577 puede aplicarse a cualquier mensaje electrónico que pueda ser transmitido a través de una red de mensajería electrónica o a través de cualquier portal electrónico. Los mensajes electrónicos pueden incluir texto, audio, vídeo, gráficos, datos y archivos adjuntos de distintos tipos. Los métodos y técnicas aquí mostradas pueden ser programados en servidores y otras computadoras y los programas de computadoras implementando la invención pueden ser grabados en medios legibles por computadora incluyendo pero no limitados a CD ROMs, RAM, discos duros y cintas magnéticas. Los Servicios de Correo Electrónico hechos-de-registro en conformidad con la presente invención pueden ser asociados con servicios de proveedores de servicio de Internet (*Internet service provider*) (ISP) para proporcionar una única solución de proveedor ISP a clientes corporativos y otros clientes institucionales. Implementar la invención descrita más arriba está al alcance de todo usuario familiarizado con la técnica de software.

Como previamente indicado, las Figuras 1-11 muestran y la especificación describe, sistemas en los cuales el servidor recibe un mensaje de un remitente y transmite este mensaje por una primera ruta a un destinatario o a un Agente de Transporte de Correo (MTA) del destinatario. Existen ocasiones en que el remitente puede desear que el servidor envíe el mensaje al destinatario o a un Agente de Transporte de Correo del destinatario por una ruta de mayor o menor recorrido, o por lo menos una ruta distinta a la primera ruta. Para lograr esto 35, el remitente etiqueta el formulario de mensaje 1200 (Fig. 14) con una indicación particular tal como "(R)" en una posición determinada como la línea de asunto del mensaje. Esta posición particular es indicada en 1202 en el formulario de mensaje 1200 en Figura 14. El paso de etiquetar "(R)" en la línea de "asunto" 1202 del mensaje es mostrada en 1206 en Figura 12.

El mensaje con la "(R)" en la linea de "asunto" es transmitido por el remitente al servidor 14, que constituye el Agente de Transporte de Correo del remitente. Esto es indicado en 1208 en la Figura 12. Como se indica en 1210, el servidor realiza un escaneo de la linea de "asunto" para determinar si existe una "(R)" en la línea, si la respuesta es "No" (ver 1211), el servidor transmite el mensaje al destinatario o al Agente de Transporte de Correo del destinatario a través de la ruta mostrada en las Figuras 1-11 e indicada en Figura 12 como "la ruta normal" y discutida antes en la especificación. Esto es indicado en 1212 en la Figura 12. Si la respuesta es "Si" (ver 1213), el mensaje es transmitido a través de una ruta de red especial como se indica en 1214 en la Figura 12.

La Figura 13 es idéntica en un número de aspectos a la Figura 12. Sin embargo, la Figura 13 incluye bloques adicionales para realizar funciones adicionales distintas a las mostradas en la Figura 12. Estas incluyen sin limitarse, lo siguiente.

(1) El remitente puede desear que una copia del mensaje sea archivada. Esto se puede obtener agregando un código tal como el número "1" después de "(R)" en la línea de "asunto" de forma tal que el código es "R1".

(2) El remitente puede desear que un registro de la transmisión sea registrado por el servidor 14 constituyendo el agente de transporte de correo del remitente. Esto se puede obtener proporcionando un código tal como "(R2)" en la línea de asunto del mensaje.

(3) El remitente puede desear que un registro de la transmisión del mensaje sea registrado en una base de datos. Esto se puede obtener al proporcionar un código tal como "(R3)" en la linea de asunto ("subject") del mensaje.

(4) El remitente puede desear que un registro de la transmisión del mensaje sea registrado en una base de datos con una anotación especial o referencia adicional. Esto se puede obtener al proporcionar un código tal como "(R4)" en la linea de asunto del mensaje.

La Figura 13 proporciona un método donde el servidor que constituye el Agente de Transporte de Correo del remitente procesa mensajes de correo electrónico seleccionados tales como aquellos especificados en este párrafo.

La Figura 13 es particularmente limitada a un código "(xyz)" en la línea de "asunto" ("subject") del mensaje. En la Figura 13, el remitente es mostrado en 1300 redactando un mensaje electrónico que incluye "(xyz)" en la línea de "asunto" del mensaje. Como se indica en 1210 en las Figuras 12 y 13, el servidor 14 que constituye el agente de transporte de correo, realiza un escaneo de la línea de "asunto" en el mensaje saliente. Si la línea de "asunto" en el mensaje no contiene el código "(R)", el servidor transmite el mensaje a través de la ruta mostrada en la Figura 1-11 y expuesta más arriba (ver 1212 en las Figuras 12 y 13). Si el código "(R)" es detectado por el servidor en la línea de "asunto" del mensaje, el servidor transmite el mensaje por una ruta de red especial como se indica en 1214 en las Figuras 12 y 13.

La Figura 13 indica en 1304 que el código "(xyz)" es removido por el servidor de la línea de "asunto" del mensaje. Si el delimitador "xyz" es detectado, una copia del mensaje es salvada. Esto es indicado en 1306 en la Figura 13. Si el delimitador "xyz" no es identificado, no será salvada una copia del mensaje.

A pesar de que la presente invención ha sido entonces descrita en detalle con respecto a las personificaciones preferidas y a los dibujos relacionados, debe ser evidente para aquellos expertos en la técnica que se pueden realizar varias adaptaciones y modificaciones a la presente invención sin apartarse del ámbito de la invención, las palabras "medios para" no estando previstas para ser interpretadas de acuerdo con 35 U.S.C. §112, párrafo 6.

REIVINDICACIONES

1. Un método para transmitir un mensaje de un remitente a una dirección de destino incluyendo los siguientes pasos:

Recibir el mensaje en un servidor (14) de parte del remitente,

Transmitir normalmente el mensaje del servidor a la dirección de destino por una primera ruta (1212), **caracterizada** por los siguientes pasos,

recibir del remitente en el servidor una indicación particular (1202), indicando que el remitente desea que el mensaje sea transmitido a la dirección de destino por una segunda ruta distinta a la primera ruta y

proporcionar la transmisión del mensaje por la segunda ruta a la dirección de destino (1214) de acuerdo con la indicación particular (1202) del remitente.

2. Un método según se establece en la reivindicación 1 donde la indicación particular (1202) es proporcionada en el mensaje del remitente por el remitente.

3. Un método según se establece en la reivindicación 2 donde la indicación particular es proporcionada en una posición particular del mensaje.

4. Un método según se establece en cualquiera de las reivindicaciones 1 a 3 donde el remitente le indica al servidor (14), con una primera adición a la indicación particular (1202), que una copia del mensaje debe ser archivada cuando el servidor transmita el mensaje por la segunda ruta a la dirección de destino y donde, de acuerdo a la primera adición a la indicación particular, el servidor (14) archiva una copia del mensaje (1306) cuando el servidor transmite el mensaje por una segunda ruta a la dirección de destino (1214).

5. Un método según se establece en cualquiera de las reivindicaciones 1 a 4 donde el remitente indica, con una segunda adición a la indicación particular (1202) que un registro de la transmisión debe ser registrado por el servidor (14) cuando el servidor transmite el mensaje por una segunda ruta a la dirección de destino y donde de acuerdo con la segunda adición a la indicación particular, el servidor (14) registra un registro de la transmisión cuando el servidor transmite el mensaje por la segunda ruta a la dirección de destino (1214).

6. Un método según se establece en cualquiera de las reivindicaciones 1 a 5 donde el remitente indica que un registro de la transmisión del mensaje debe ser registrado en una base de datos cuando una tercera adición sea proporcionada a la indicación particular (1202) y cuando el servidor transmite el mensaje por la segunda ruta a la dirección de destino y donde de acuerdo con la tercera adición a la indicación particular, el servidor proporciona un registro de transmisión del mensaje en la base de datos cuando el servidor transmite el mensaje por la segunda ruta a la dirección de destino (1214).

7. Un método según se establece en cualquiera de las reivindicaciones 1 a 6 donde el remitente indica que la transmisión del mensaje debe ser registrada en una base de datos con una anotación especial cuando una cuarta adición es proporcionada a la indicación particular (1202) y cuando el mensaje es transmitido por el servidor (14) por la segunda ruta a la dirección de destino y donde el servidor (14) registra la transmisión de mensaje en la base de datos con una anotación especial cuando la cuarta adición es proporcionada a la indicación particular y cuando el mensaje es transmitido por el servidor por la segunda ruta a la dirección de destino (1214).

8. Un método según se establece en cualquiera de las reivindicaciones 1 a 7 donde un recibo es transmitido por el servidor (14) al remitente después de la transmisión del mensaje por el servidor a la dirección de destino; y donde el mensaje y el recibo son borrados del servidor después de la transmisión del recibo por medio del servidor al remitente (292).

9. Un método según se establece en la reivindicación 8 donde el servidor (14) crea una firma digital del recibo y transmite la firma digital con el recibo al remitente (290) y donde el servidor borra la firma digital después de la transmisión del recibo al remitente.

10. Un método según se establece en la reivindicación 9 donde el remitente transmite el recibo con la firma digital al servidor (14) cuando el remitente desea que el recibo sea autenticado y donde el servidor utilice el recibo y la firma digital del recibo para autenticar el recibo.

11. Un método según se establece en la reivindicación 10 donde el servidor obtiene una primera huella digital, un hash del recibo y descifra la firma digital para obtener una segunda huella digital, un hash, (702, 703) y donde el servidor autentica el recibo si la primera y segunda huella digital coinciden.

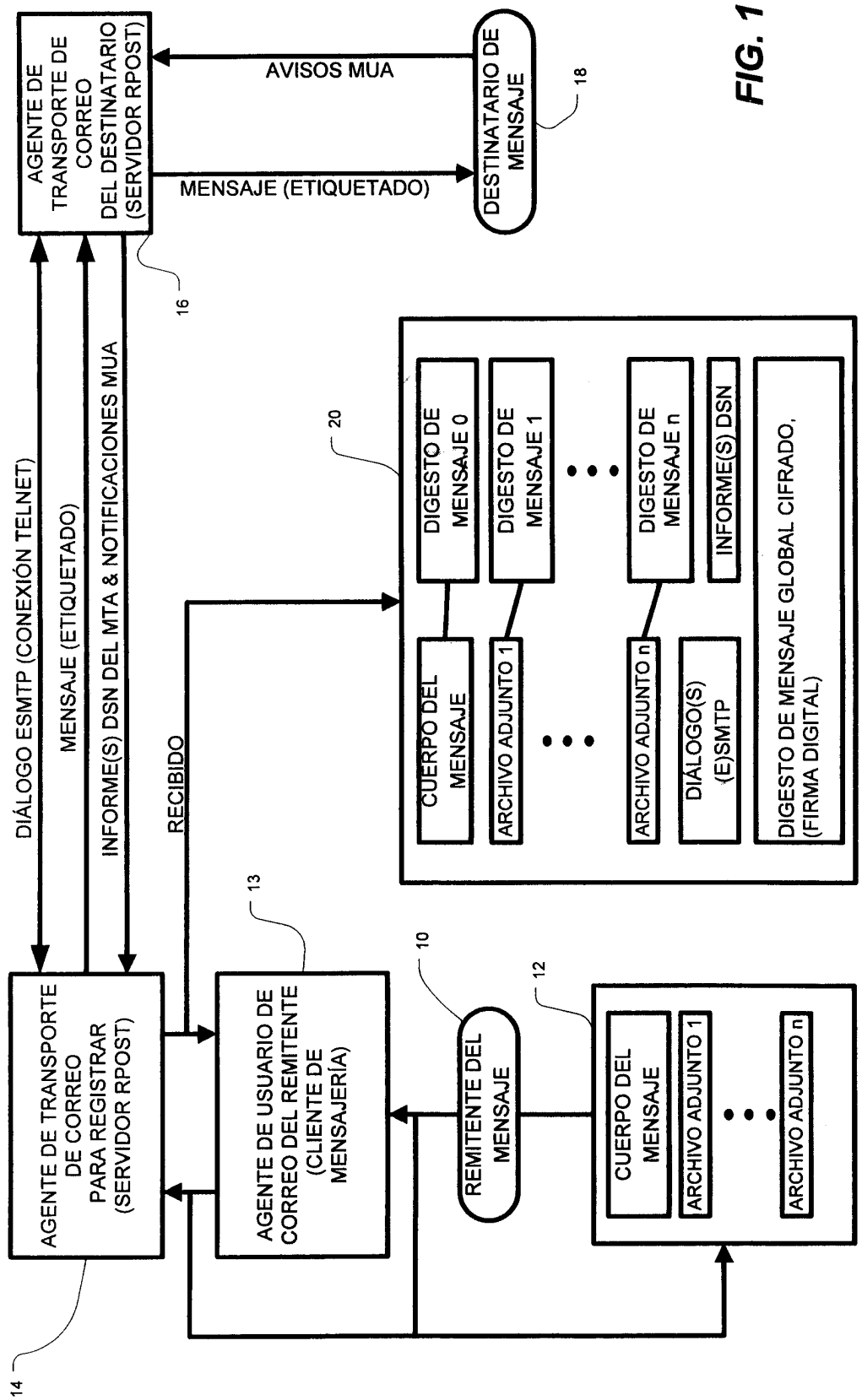
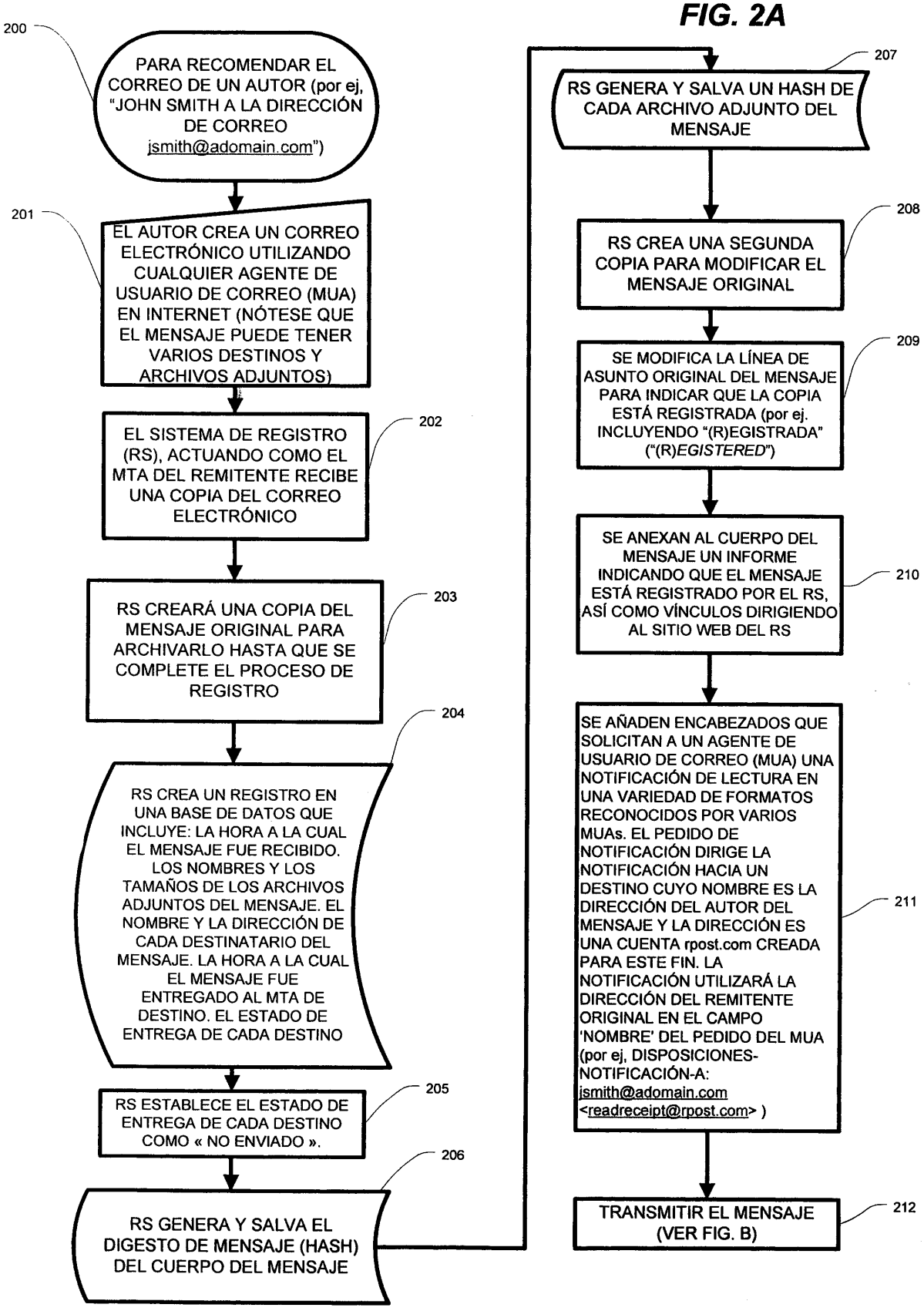

AGENTE DE TRANSPORTE DE CORREO DEL DESTINATARIO (SERVIDOR RPOST)
AVISOS MUA
MENSAJE (ETIQUETADO)
DESTINATARIO DE MENSAJE
18
16
DIÁLOGO ESMTP (CONEXIÓN TELNET)
MENSAJE (ETIQUETADO)
INFORME(S) DSN DEL MTA & NOTIFICACIONES MUA
RECIBIDO
20
DIGESTO DE MENSAJE 0
DIGESTO DE MENSAJE 1
DIGESTO DE MENSAJE n
INFORME(S) DSN
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
DIÁLOGO(S) (E)SMTP
DIGESTO DE MENSAJE GLOBAL CIFRADO, (FIRMA DIGITAL)
13
10
12
AGENTE DE TRANSPORTE DE CORREO PARA REGISTRAR (SERVIDOR RPOST)
AGENTE DE USUARIO DE CORREO DEL REMITENTE (CLIENTE DE MENSAJERÍA)
REMITENTE DEL MENSAJE
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
14

FIG. 1

FIG. 2A


200
PARA RECOMENDAR EL CORREO DE UN AUTOR (por ej, "JOHN SMITH A LA DIRECCIÓN DE CORREO jsmith@adomain.com")
201
EL AUTOR CREA UN CORREO ELECTRÓNICO UTILIZANDO CUALQUIER AGENTE DE USUARIO DE CORREO (MUA) EN INTERNET (NÓTESE QUE EL MENSAJE PUEDE TENER VARIOS DESTINOS Y ARCHIVOS ADJUNTOS)
202
EL SISTEMA DE REGISTRO (RS), ACTUANDO COMO EL MTA DEL REMITENTE RECIBE UNA COPIA DEL CORREO ELECTRÓNICO
203
RS CREARÁ UNA COPIA DEL MENSAJE ORIGINAL PARA ARCHIVARLO HASTA QUE SE COMPLETE EL PROCESO DE REGISTRO
204
RS CREA UN REGISTRO EN UNA BASE DE DATOS QUE INCLUYE: LA HORA A LA CUAL EL MENSAJE FUE RECIBIDO. LOS NOMBRES Y LOS TAMAÑOS DE LOS ARCHIVOS ADJUNTOS DEL MENSAJE. EL NOMBRE Y LA DIRECCIÓN DE CADA DESTINATARIO DEL MENSAJE. LA HORA A LA CUAL EL MENSAJE FUE ENTREGADO AL MTA DE DESTINO. EL ESTADO DE ENTREGA DE CADA DESTINO
205
RS ESTABLECE EL ESTADO DE ENTREGA DE CADA DESTINO COMO « NO ENVIADO ».
206
RS GENERA Y SALVA EL DIGESTO DE MENSAJE (HASH) DEL CUERPO DEL MENSAJE
207
RS GENERA Y SALVA UN HASH DE CADA ARCHIVO ADJUNTO DEL MENSAJE
208
RS CREA UNA SEGUNDA COPIA PARA MODIFICAR EL MENSAJE ORIGINAL
209
SE MODIFICA LA LÍNEA DE ASUNTO ORIGINAL DEL MENSAJE PARA INDICAR QUE LA COPIA ESTÁ REGISTRADA (por ej. INCLUYENDO "(R)EGISTRADA" ("(R)EGISTERED")
210
SE ANEXAN AL CUERPO DEL MENSAJE UN INFORME INDICANDO QUE EL MENSAJE ESTÁ REGISTRADO POR EL RS, ASÍ COMO VÍNCULOS DIRIGIENDO AL SITIO WEB DEL RS
211
SE AÑADEN ENCABEZADOS QUE SOLICITAN A UN AGENTE DE USUARIO DE CORREO (MUA) UNA NOTIFICACIÓN DE LECTURA EN UNA VARIEDAD DE FORMATOS RECONOCIDOS POR VARIOS MUAs. EL PEDIDO DE NOTIFICACIÓN DIRIGE LA NOTIFICACIÓN HACIA UN DESTINO CUYO NOMBRE ES LA DIRECCIÓN DEL AUTOR DEL MENSAJE Y LA DIRECCIÓN ES UNA CUENTA rpost.com CREADA PARA ESTE FIN. LA NOTIFICACIÓN UTILIZARÁ LA DIRECCIÓN DEL REMITENTE ORIGINAL EN EL CAMPO 'NOMBRE' DEL PEDIDO DEL MUA (por ej, DISPOSICIONES-NOTIFICACIÓN-A: jsmith@adomain.com <readreceipt@rpost.com>)
212
TRANSMITIR EL MENSAJE (VER FIG. B)

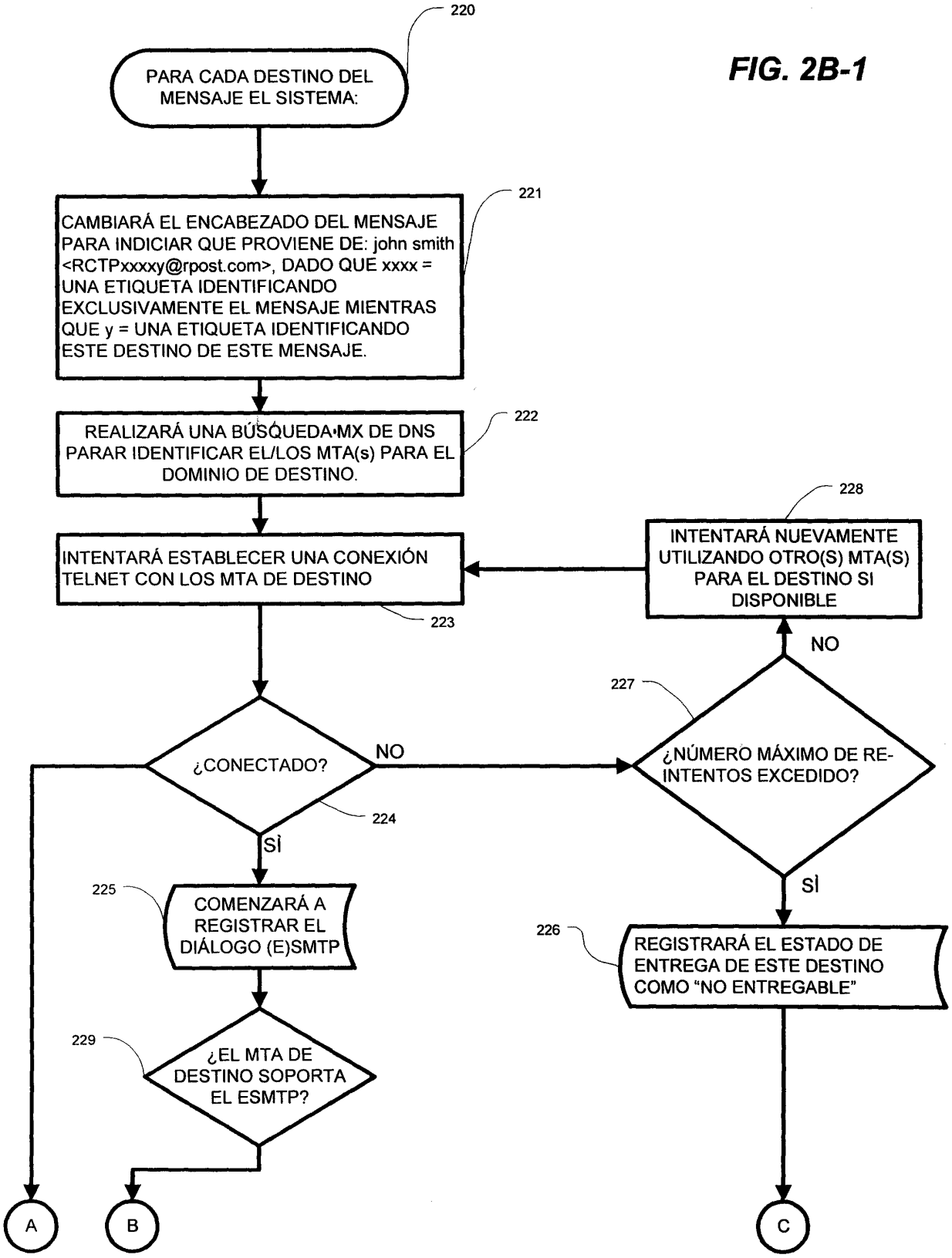

220
PARA CADA DESTINO DEL MENSAJE EL SISTEMA:
221
CAMBIARÁ EL ENCABEZADO DEL MENSAJE PARA INDICIAR QUE PROVIENE DE: john smith <RCTPxxxxy@rpost.com>, DADO QUE xxxx = UNA ETIQUETA IDENTIFICANDO EXCLUSIVAMENTE EL MENSAJE MIENTRAS QUE y = UNA ETIQUETA IDENTIFICANDO ESTE DESTINO DE ESTE MENSAJE.
222
REALIZARÁ UNA BÚSQUEDA MX DE DNS PARAR IDENTIFICAR EL/LOS MTA(s) PARA EL DOMINIO DE DESTINO.
INTENTARÁ ESTABLECER UNA CONEXIÓN TELNET CON LOS MTA DE DESTINO
223
228
INTENTARÁ NUEVAMENTE UTILIZANDO OTRO(S) MTA(S) PARA EL DESTINO SI DISPONIBLE
NO
227
¿CONECTADO?
NO
¿NÚMERO MÁXIMO DE RE-INTENTOS EXCEDIDO?
224
SÍ
SÍ
225
COMENZARÁ A REGISTRAR EL DIÁLOGO (E)SMTP
226
REGISTRARÁ EL ESTADO DE ENTREGA DE ESTE DESTINO COMO "NO ENTREGABLE"
229
¿EL MTA DE DESTINO SOPORTA EL ESMTP?
A
B
C

FIG. 2B-1

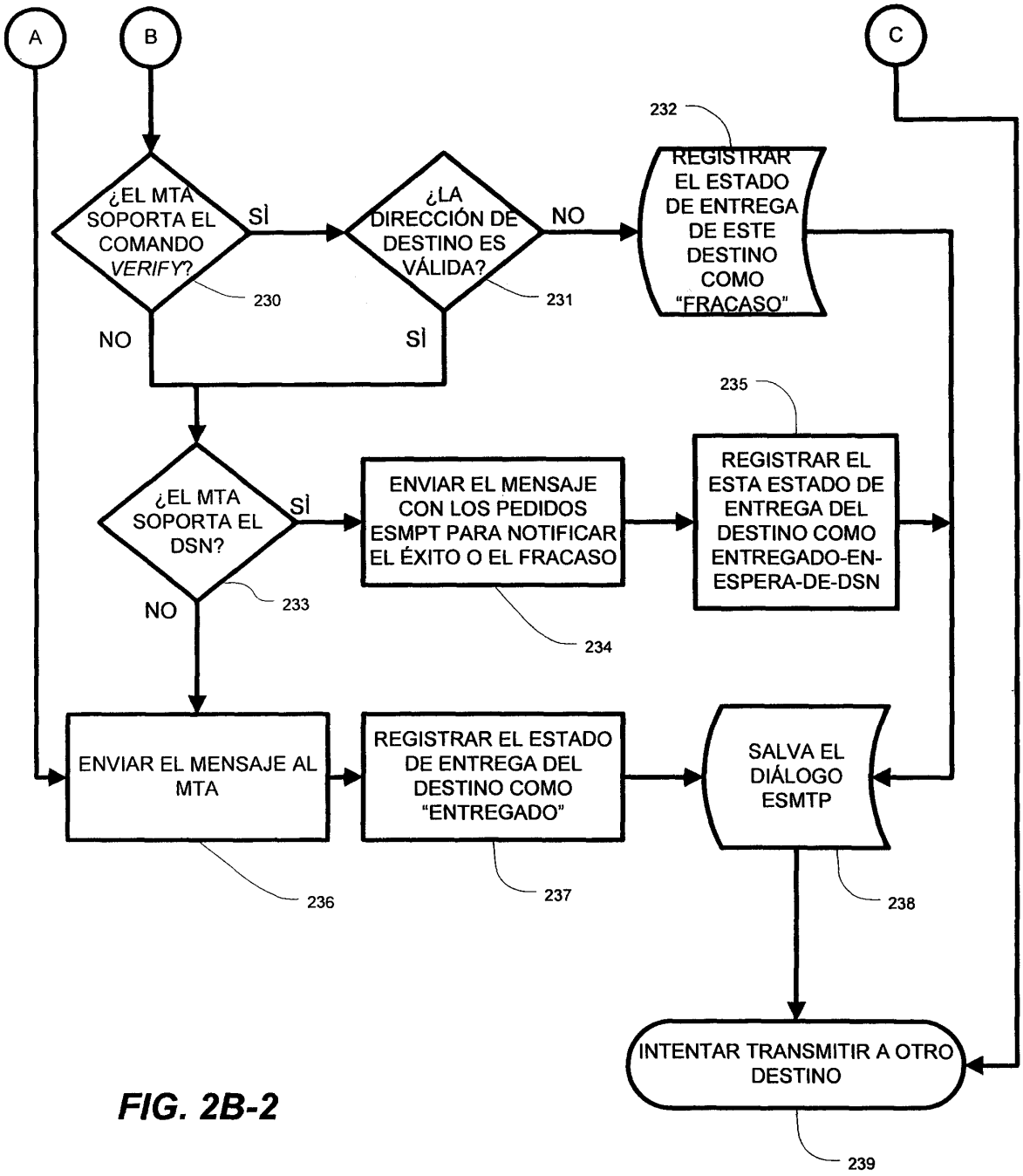

A
B
C
¿EL MTA SOPORTA EL COMANDO *VERIFY*?
SÍ
NO
230
¿LA DIRECCIÓN DE DESTINO ES VÁLIDA?
NO
SÍ
231
232
REGISTRAR EL ESTADO DE ENTREGA DE ESTE DESTINO COMO "FRACASO"
¿EL MTA SOPORTA EL DSN?
SÍ
NO
233
ENVIAR EL MENSAJE CON LOS PEDIDOS ESMPT PARA NOTIFICAR EL ÉXITO O EL FRACASO
234
235
REGISTRAR EL ESTA ESTADO DE ENTREGA DEL DESTINO COMO ENTREGADO-EN-ESPERA-DE-DSN
ENVIAR EL MENSAJE AL MTA
236
REGISTRAR EL ESTADO DE ENTREGA DEL DESTINO COMO "ENTREGADO"
237
SALVA EL DIÁLOGO ESMTP
238
INTENTAR TRANSMITIR A OTRO DESTINO
239

FIG. 2B-2

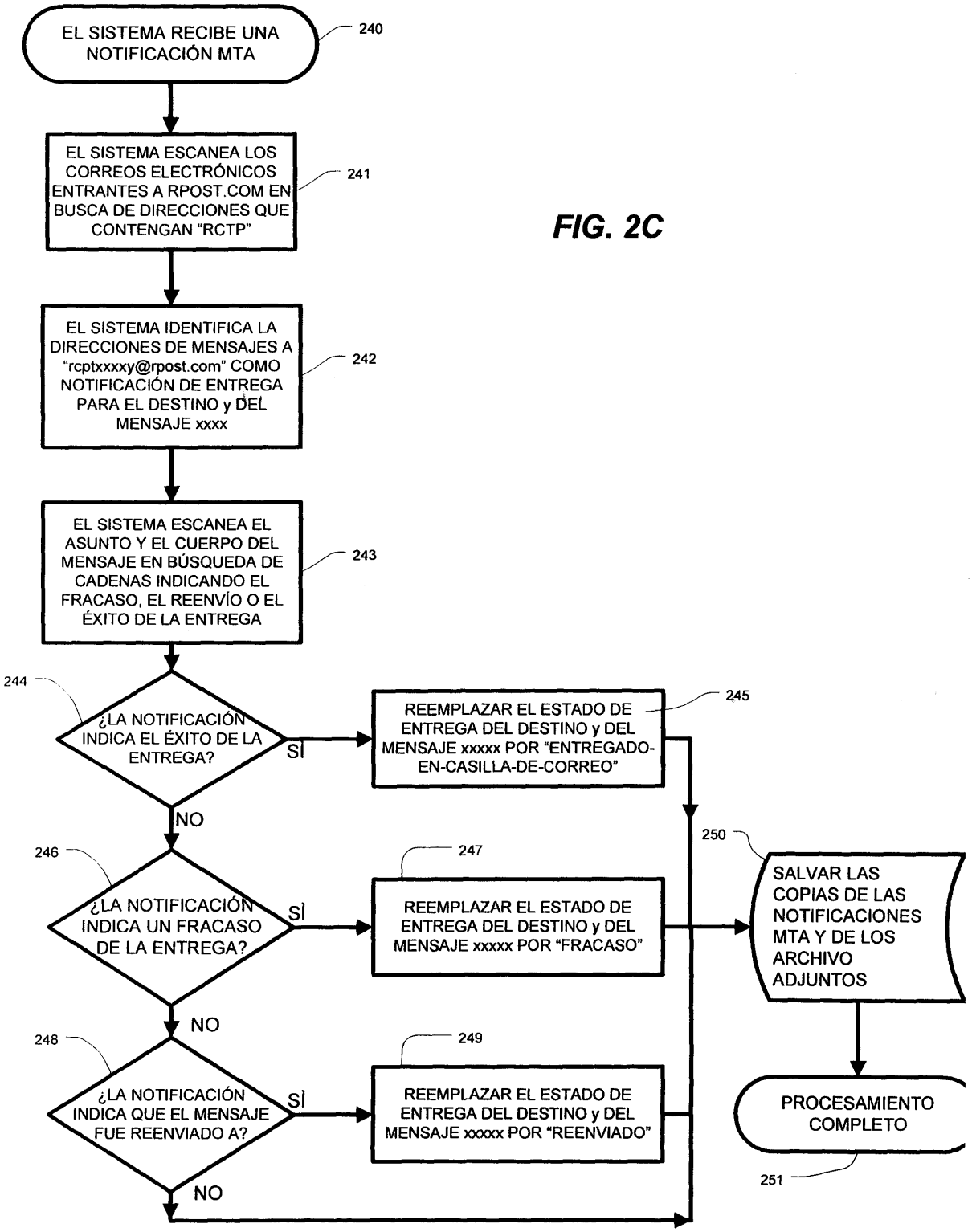

EL SISTEMA RECIBE UNA NOTIFICACIÓN MTA
240
EL SISTEMA ESCANEA LOS CORREOS ELECTRÓNICOS ENTRANTES A RPOST.COM EN BUSCA DE DIRECCIONES QUE CONTENGAN "RCTP"
241
EL SISTEMA IDENTIFICA LA DIRECCIONES DE MENSAJES A "rcptxxxxy@rpost.com" COMO NOTIFICACIÓN DE ENTREGA PARA EL DESTINO y DEL MENSAJE xxxx
242
EL SISTEMA ESCANEA EL ASUNTO Y EL CUERPO DEL MENSAJE EN BÚSQUEDA DE CADENAS INDICANDO EL FRACASO, EL REENVÍO O EL ÉXITO DE LA ENTREGA
243
244
¿LA NOTIFICACIÓN INDICA EL ÉXITO DE LA ENTREGA?
SÍ
REEMPLAZAR EL ESTADO DE ENTREGA DEL DESTINO y DEL MENSAJE xxxxx POR "ENTREGADO-EN-CASILLA-DE-CORREO"
245
NO
246
¿LA NOTIFICACIÓN INDICA UN FRACASO DE LA ENTREGA?
SÍ
247
REEMPLAZAR EL ESTADO DE ENTREGA DEL DESTINO y DEL MENSAJE xxxxx POR "FRACASO"
NO
248
¿LA NOTIFICACIÓN INDICA QUE EL MENSAJE FUE REENVIADO A?
SÍ
249
REEMPLAZAR EL ESTADO DE ENTREGA DEL DESTINO y DEL MENSAJE xxxxx POR "REENVIADO"
NO
250
SALVAR LAS COPIAS DE LAS NOTIFICACIONES MTA Y DE LOS ARCHIVO ADJUNTOS
PROCESAMIENTO COMPLETO
251

FIG. 2C

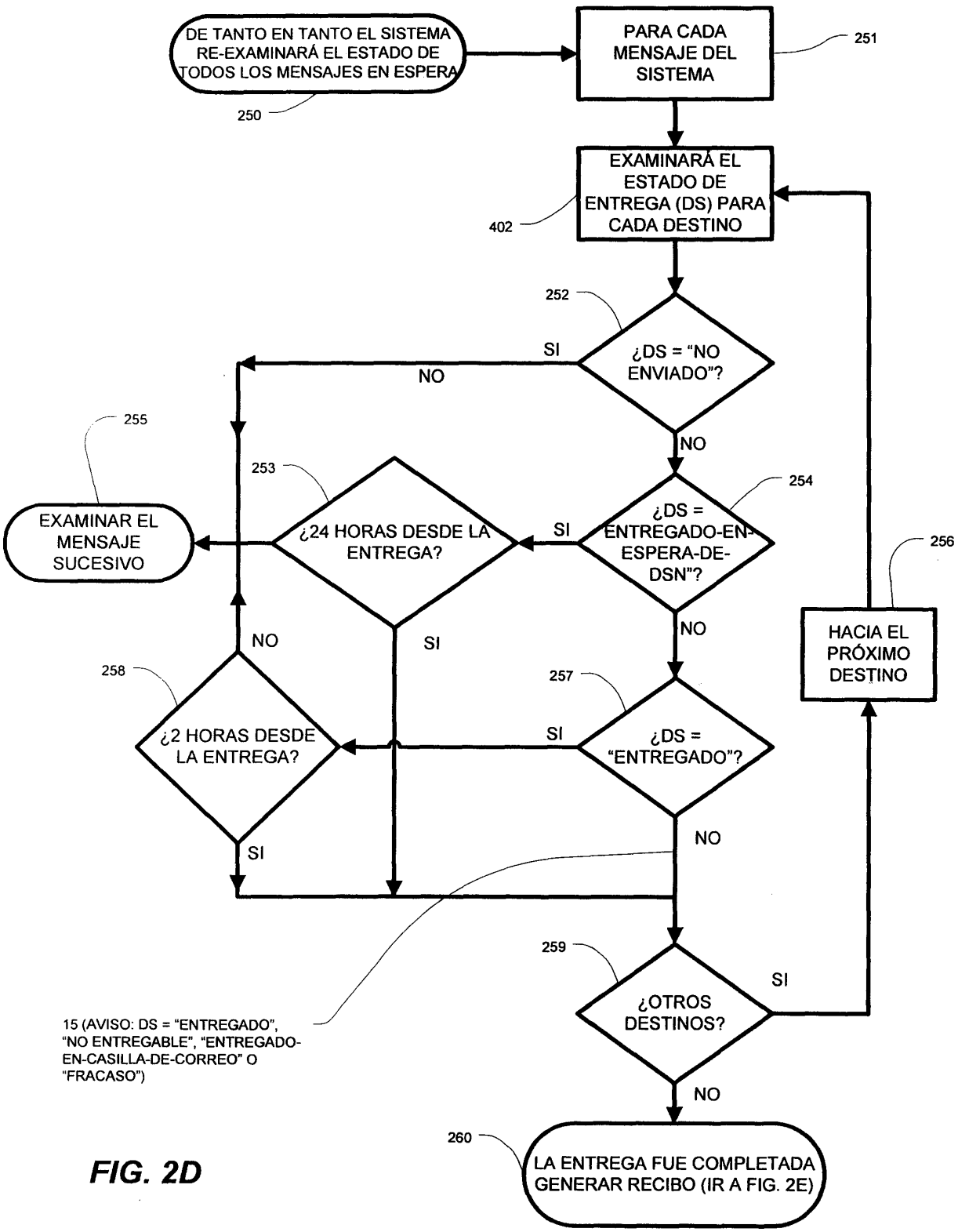
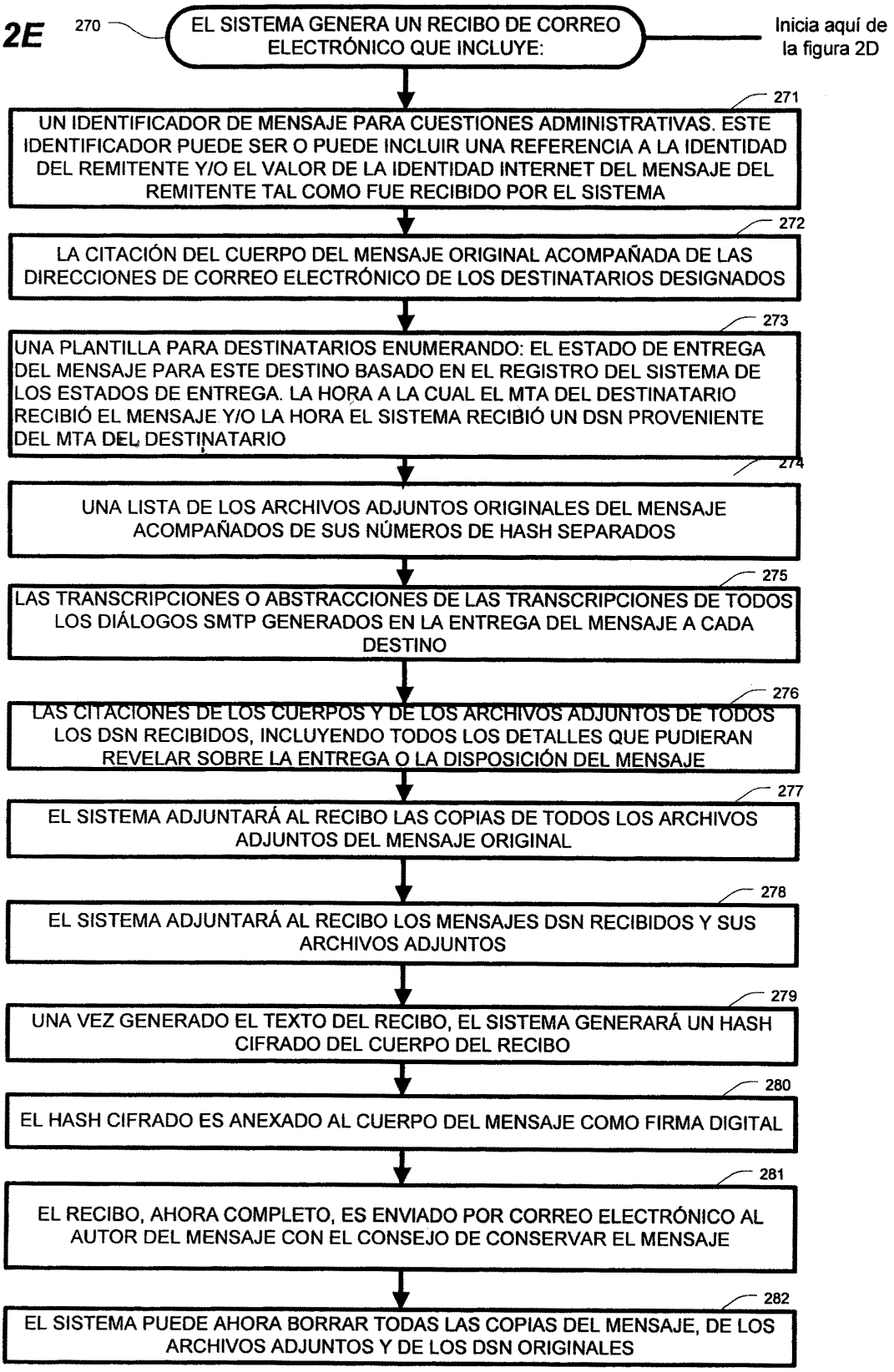

DE TANTO EN TANTO EL SISTEMA RE-EXAMINARÁ EL ESTADO DE TODOS LOS MENSAJES EN ESPERA
250
PARA CADA MENSAJE DEL SISTEMA
251
EXAMINARÁ EL ESTADO DE ENTREGA (DS) PARA CADA DESTINO
402
252
¿DS = "NO ENVIADO"?
SI
NO
255
EXAMINAR EL MENSAJE SUCESIVO
253
¿24 HORAS DESDE LA ENTREGA?
SI
NO
254
¿DS = ENTREGADO-EN-ESPERA-DE-DSN"?
NO
256
HACIA EL PRÓXIMO DESTINO
258
¿2 HORAS DESDE LA ENTREGA?
NO
SI
257
¿DS = "ENTREGADO"?
SI
NO
259
¿OTROS DESTINOS?
SI
NO
260
LA ENTREGA FUE COMPLETADA GENERAR RECIBO (IR A FIG. 2E)
15 (AVISO: DS = "ENTREGADO", "NO ENTREGABLE", "ENTREGADO-EN-CASILLA-DE-CORREO" O "FRACASO")

FIG. 2D

FIG. 2E


270
EL SISTEMA GENERA UN RECIBO DE CORREO ELECTRÓNICO QUE INCLUYE:
Inicia aquí de la figura 2D
271
UN IDENTIFICADOR DE MENSAJE PARA CUESTIONES ADMINISTRATIVAS. ESTE IDENTIFICADOR PUEDE SER O PUEDE INCLUIR UNA REFERENCIA A LA IDENTIDAD DEL REMITENTE Y/O EL VALOR DE LA IDENTIDAD INTERNET DEL MENSAJE DEL REMITENTE TAL COMO FUE RECIBIDO POR EL SISTEMA
272
LA CITACIÓN DEL CUERPO DEL MENSAJE ORIGINAL ACOMPAÑADA DE LAS DIRECCIONES DE CORREO ELECTRÓNICO DE LOS DESTINATARIOS DESIGNADOS
273
UNA PLANTILLA PARA DESTINATARIOS ENUMERANDO: EL ESTADO DE ENTREGA DEL MENSAJE PARA ESTE DESTINO BASADO EN EL REGISTRO DEL SISTEMA DE LOS ESTADOS DE ENTREGA. LA HORA A LA CUAL EL MTA DEL DESTINATARIO RECIBIÓ EL MENSAJE Y/O LA HORA EL SISTEMA RECIBIÓ UN DSN PROVENIENTE DEL MTA DEL DESTINATARIO
274
UNA LISTA DE LOS ARCHIVOS ADJUNTOS ORIGINALES DEL MENSAJE ACOMPAÑADOS DE SUS NÚMEROS DE HASH SEPARADOS
275
LAS TRANSCRIPCIONES O ABSTRACCIONES DE LAS TRANSCRIPCIONES DE TODOS LOS DIÁLOGOS SMTP GENERADOS EN LA ENTREGA DEL MENSAJE A CADA DESTINO
276
LAS CITACIONES DE LOS CUERPOS Y DE LOS ARCHIVOS ADJUNTOS DE TODOS LOS DSN RECIBIDOS, INCLUYENDO TODOS LOS DETALLES QUE PUDIERAN REVELAR SOBRE LA ENTREGA O LA DISPOSICIÓN DEL MENSAJE
277
EL SISTEMA ADJUNTARÁ AL RECIBO LAS COPIAS DE TODOS LOS ARCHIVOS ADJUNTOS DEL MENSAJE ORIGINAL
278
EL SISTEMA ADJUNTARÁ AL RECIBO LOS MENSAJES DSN RECIBIDOS Y SUS ARCHIVOS ADJUNTOS
279
UNA VEZ GENERADO EL TEXTO DEL RECIBO, EL SISTEMA GENERARÁ UN HASH CIFRADO DEL CUERPO DEL RECIBO
280
EL HASH CIFRADO ES ANEXADO AL CUERPO DEL MENSAJE COMO FIRMA DIGITAL
281
EL RECIBO, AHORA COMPLETO, ES ENVIADO POR CORREO ELECTRÓNICO AL AUTOR DEL MENSAJE CON EL CONSEJO DE CONSERVAR EL MENSAJE
282
EL SISTEMA PUEDE AHORA BORRAR TODAS LAS COPIAS DEL MENSAJE, DE LOS ARCHIVOS ADJUNTOS Y DE LOS DSN ORIGINALES

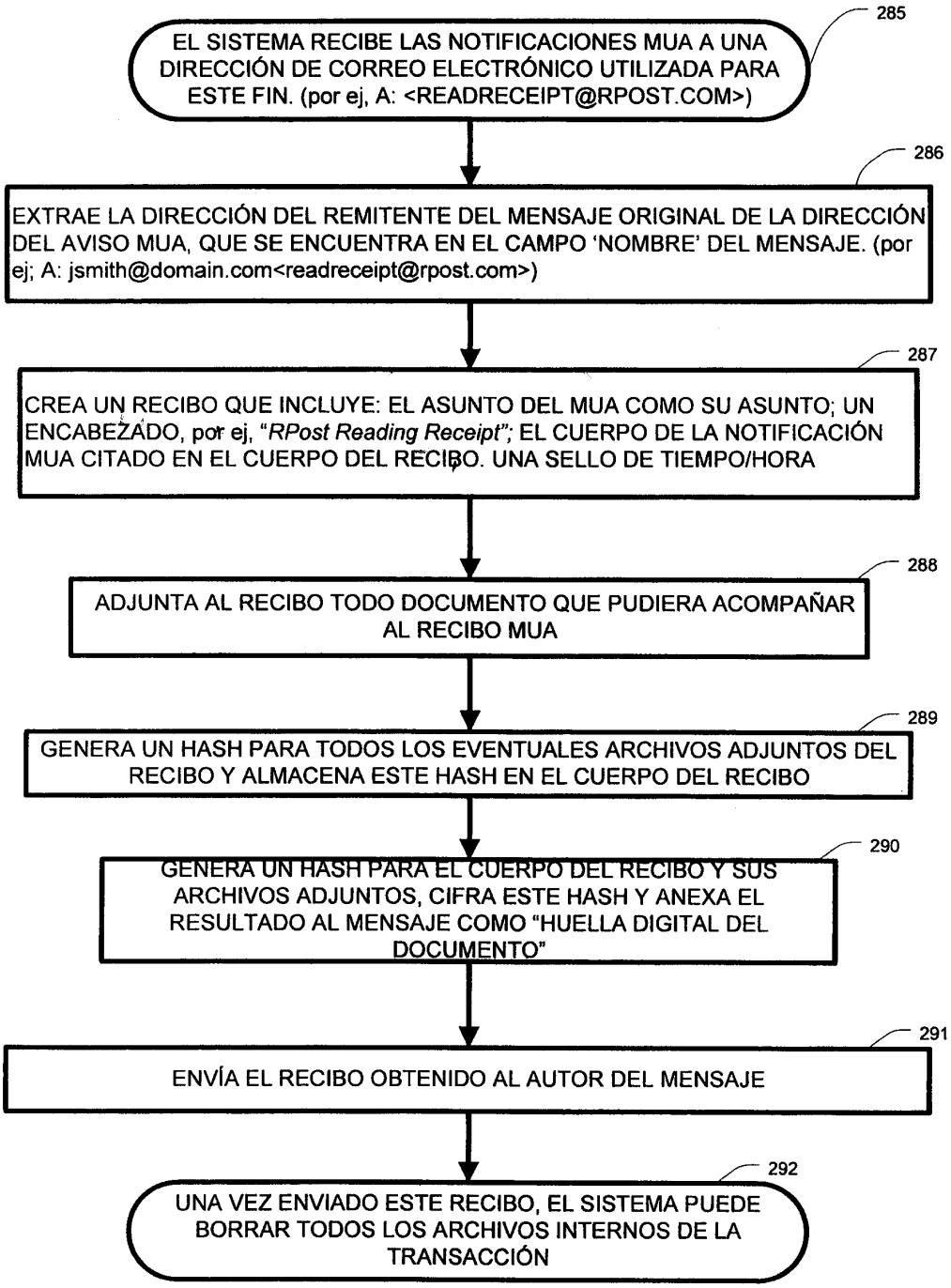

285
EL SISTEMA RECIBE LAS NOTIFICACIONES MUA A UNA DIRECCIÓN DE CORREO ELECTRÓNICO UTILIZADA PARA ESTE FIN. (por ej, A: <READRECEIPT@RPOST.COM>)
286
EXTRAE LA DIRECCIÓN DEL REMITENTE DEL MENSAJE ORIGINAL DE LA DIRECCIÓN DEL AVISO MUA, QUE SE ENCUENTRA EN EL CAMPO 'NOMBRE' DEL MENSAJE. (por ej; A: jsmith@domain.com<readreceipt@rpost.com>)
287
CREA UN RECIBO QUE INCLUYE: EL ASUNTO DEL MUA COMO SU ASUNTO; UN ENCABEZADO, por ej, "*RPost Reading Receipt*"; EL CUERPO DE LA NOTIFICACIÓN MUA CITADO EN EL CUERPO DEL RECIBO. UNA SELLO DE TIEMPO/HORA
288
ADJUNTA AL RECIBO TODO DOCUMENTO QUE PUDIERA ACOMPAÑAR AL RECIBO MUA
289
GENERA UN HASH PARA TODOS LOS EVENTUALES ARCHIVOS ADJUNTOS DEL RECIBO Y ALMACENA ESTE HASH EN EL CUERPO DEL RECIBO
290
GENERA UN HASH PARA EL CUERPO DEL RECIBO Y SUS ARCHIVOS ADJUNTOS, CIFRA ESTE HASH Y ANEXA EL RESULTADO AL MENSAJE COMO "HUELLA DIGITAL DEL DOCUMENTO"
291
ENVÍA EL RECIBO OBTENIDO AL AUTOR DEL MENSAJE
292
UNA VEZ ENVIADO ESTE RECIBO, EL SISTEMA PUEDE BORRAR TODOS LOS ARCHIVOS INTERNOS DE LA TRANSACCIÓN

FIG. 2F

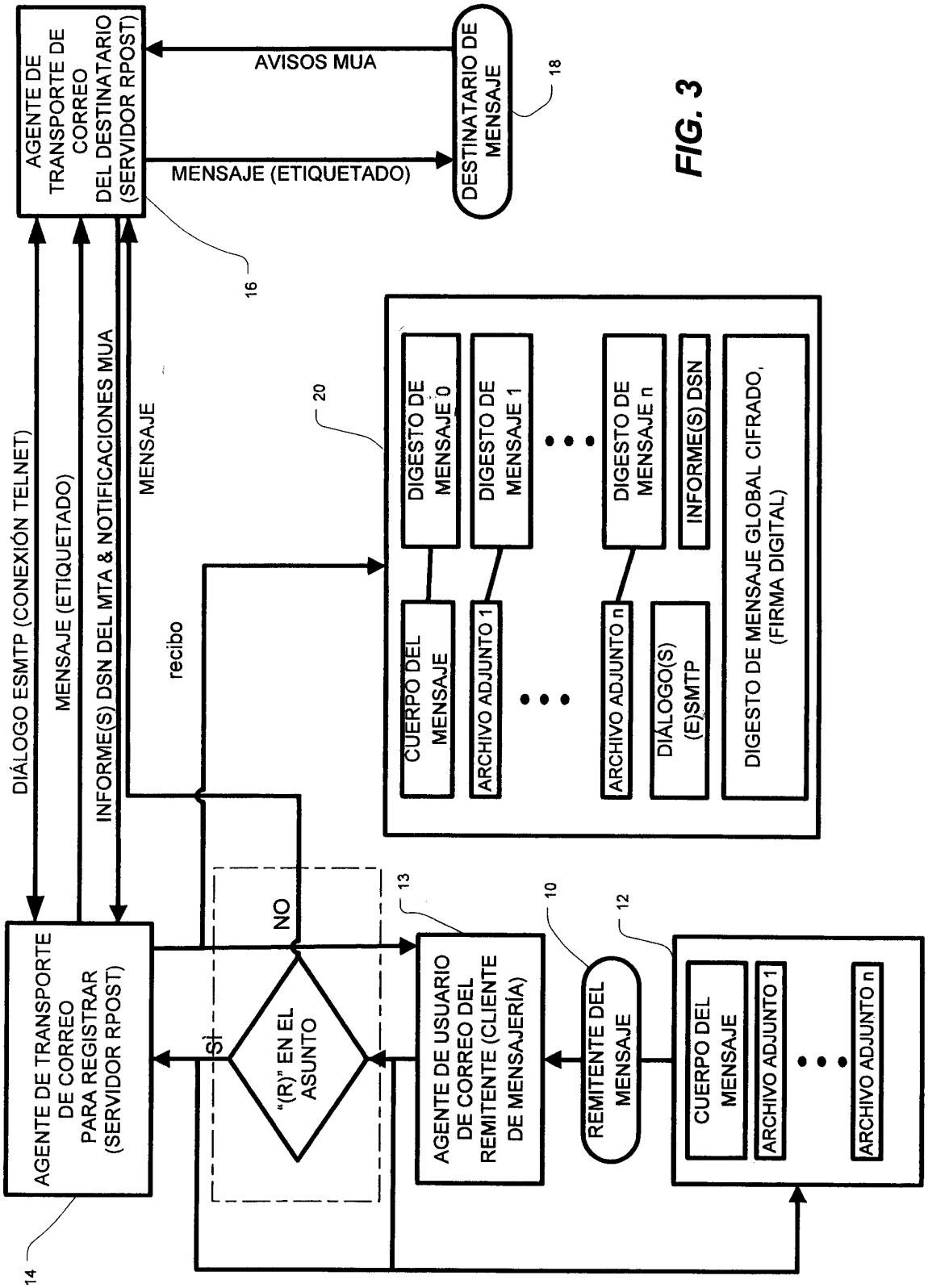

AGENTE DE TRANSPORTE DE CORREO DEL DESTINATARIO (SERVIDOR RPOST)
AVISOS MUA
MENSAJE (ETIQUETADO)
DESTINATARIO DE MENSAJE
18
16
DIÁLOGO ESMTP (CONEXIÓN TELNET)
MENSAJE (ETIQUETADO)
INFORME(S) DSN DEL MTA & NOTIFICACIONES MUA
MENSAJE
recibo
20
DIGESTO DE MENSAJE 0
DIGESTO DE MENSAJE 1
DIGESTO DE MENSAJE n
INFORME(S) DSN
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
DIÁLOGO(S) (E)SMTP
DIGESTO DE MENSAJE GLOBAL CIFRADO, (FIRMA DIGITAL)
NO
SI
"(R)" EN EL ASUNTO
13
AGENTE DE USUARIO DE CORREO DEL REMITENTE (CLIENTE DE MENSAJERÍA)
10
REMITENTE DEL MENSAJE
12
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
AGENTE DE TRANSPORTE DE CORREO PARA REGISTRAR (SERVIDOR RPOST)
14

FIG. 3

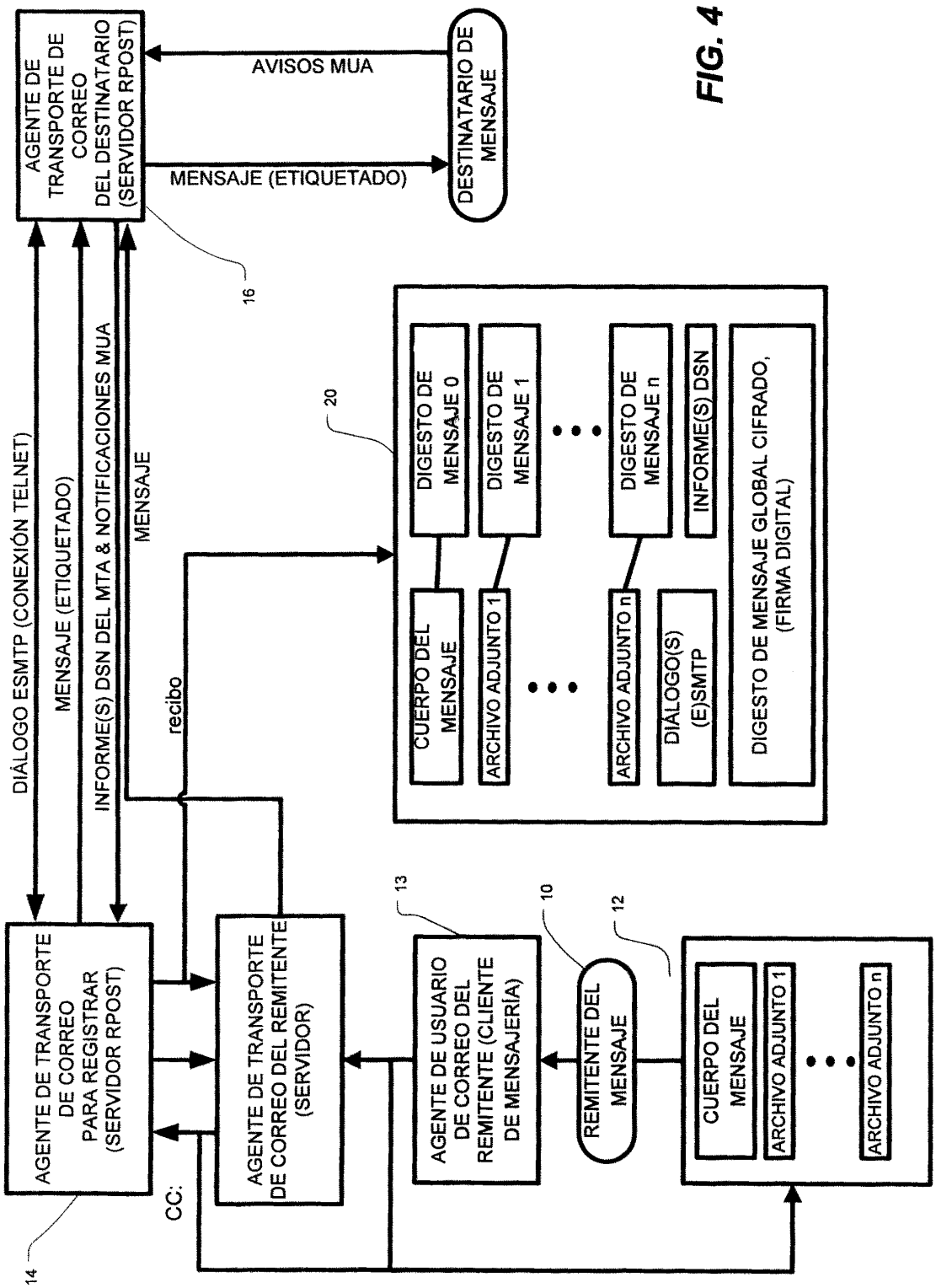

AGENTE DE TRANSPORTE DE CORREO DEL DESTINATARIO (SERVIDOR RPOST)
AVISOS MUA
DESTINATARIO DE MENSAJE
MENSAJE (ETIQUETADO)
16
DIÁLOGO ESMTP (CONEXIÓN TELNET)
MENSAJE (ETIQUETADO)
INFORME(S) DSN DEL MTA & NOTIFICACIONES MUA
MENSAJE
recibo
20
DIGESTO DE MENSAJE 0
DIGESTO DE MENSAJE 1
DIGESTO DE MENSAJE n
INFORME(S) DSN
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
DIÁLOGO(S) (E)SMTP
DIGESTO DE MENSAJE GLOBAL CIFRADO, (FIRMA DIGITAL)
AGENTE DE TRANSPORTE DE CORREO PARA REGISTRAR (SERVIDOR RPOST)
AGENTE DE TRANSPORTE DE CORREO DEL REMITENTE (SERVIDOR)
CC:
AGENTE DE USUARIO DE CORREO DEL REMITENTE (CLIENTE DE MENSAJERÍA)
REMITENTE DEL MENSAJE
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
13
10
12
14

FIG. 4

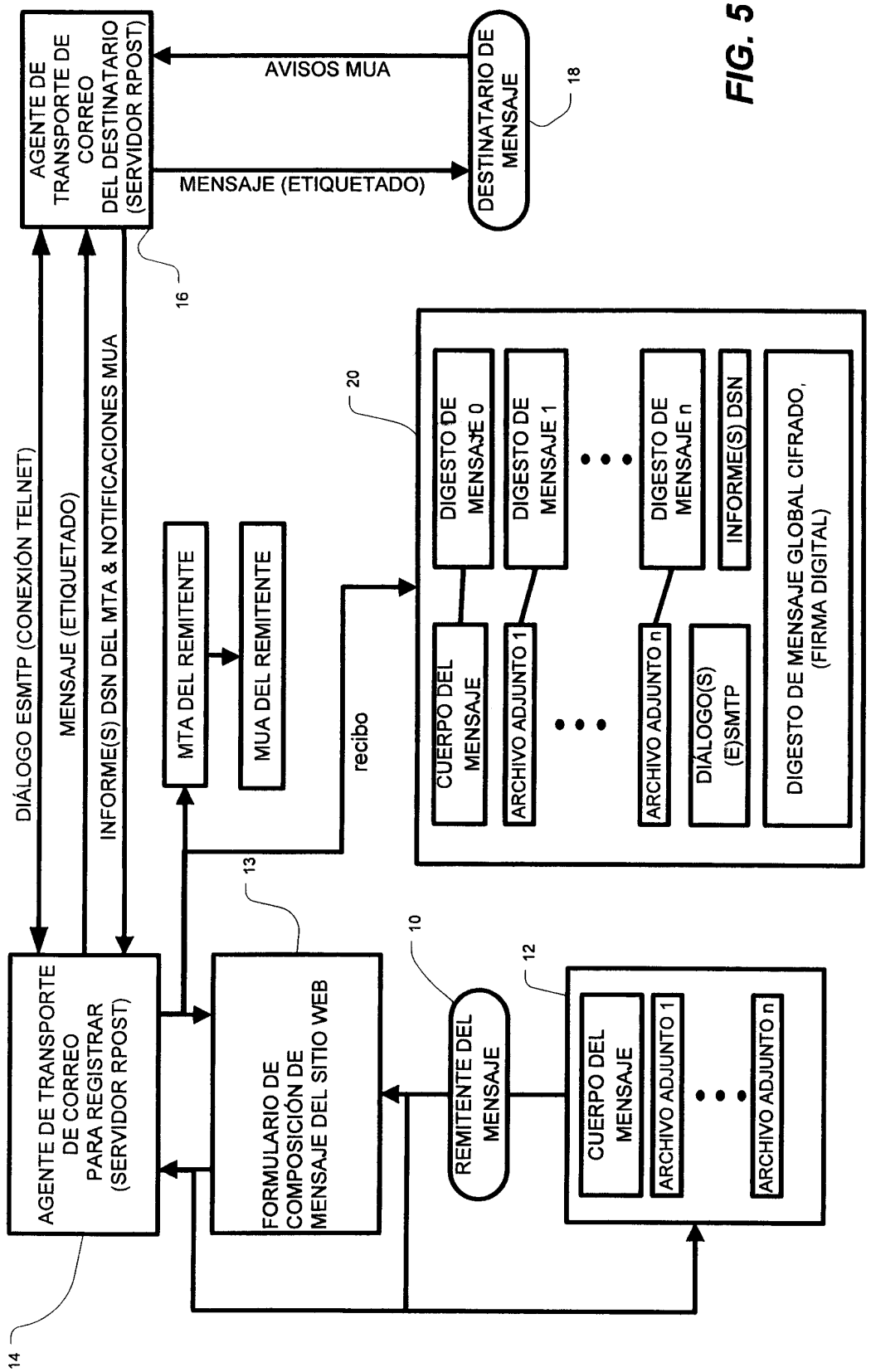

AGENTE DE TRANSPORTE DE CORREO DEL DESTINATARIO (SERVIDOR RPOST)
AVISOS MUA
MENSAJE (ETIQUETADO)
DESTINATARIO DE MENSAJE
18
16
DIÁLOGO ESMTP (CONEXIÓN TELNET)
MENSAJE (ETIQUETADO)
INFORME(S) DSN DEL MTA & NOTIFICACIONES MUA
MTA DEL REMITENTE
MUA DEL REMITENTE
recibo
20
DIGESTO DE MENSAJE 0
DIGESTO DE MENSAJE 1
DIGESTO DE MENSAJE n
INFORME(S) DSN
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
DIÁLOGO(S) (E)SMTP
DIGESTO DE MENSAJE GLOBAL CIFRADO, (FIRMA DIGITAL)
13
10
12
AGENTE DE TRANSPORTE DE CORREO PARA REGISTRAR (SERVIDOR RPOST)
FORMULARIO DE COMPOSICIÓN DE MENSAJE DEL SITIO WEB
REMITENTE DEL MENSAJE
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
14

FIG. 5

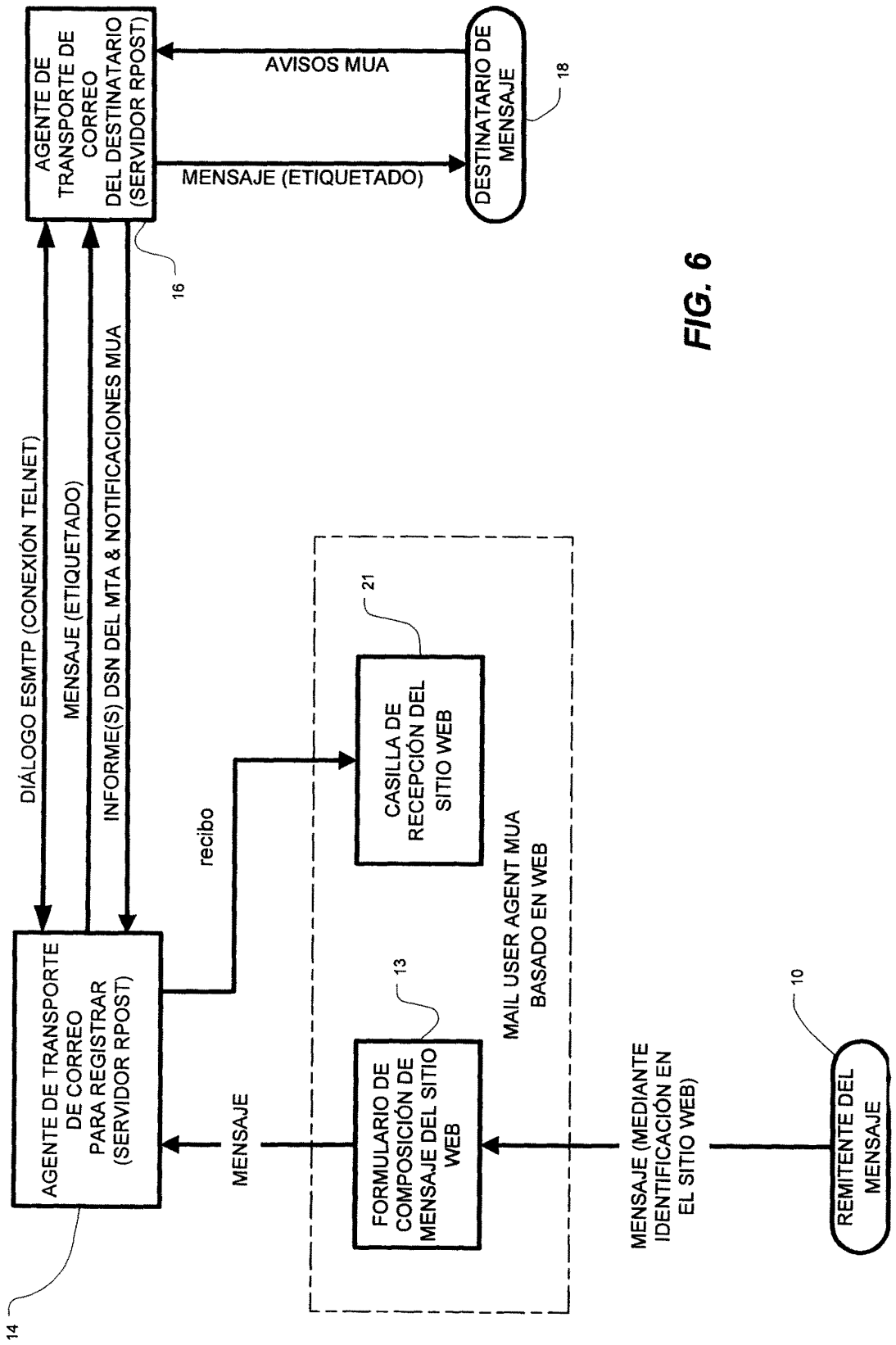

AGENTE DE TRANSPORTE DE CORREO DEL DESTINATARIO (SERVIDOR RPOST)
AVISOS MUA
MENSAJE (ETIQUETADO)
DESTINATARIO DE MENSAJE
18
16
DIÁLOGO ESMTP (CONEXIÓN TELNET)
MENSAJE (ETIQUETADO)
INFORME(S) DSN DEL MTA & NOTIFICACIONES MUA
recibo
21
CASILLA DE RECEPCIÓN DEL SITIO WEB
MAIL USER AGENT MUA BASADO EN WEB
13
AGENTE DE TRANSPORTE DE CORREO PARA REGISTRAR (SERVIDOR RPOST)
MENSAJE
FORMULARIO DE COMPOSICIÓN DE MENSAJE DEL SITIO WEB
MENSAJE (MEDIANTE IDENTIFICACIÓN EN EL SITIO WEB)
10
REMITENTE DEL MENSAJE
14

FIG. 6

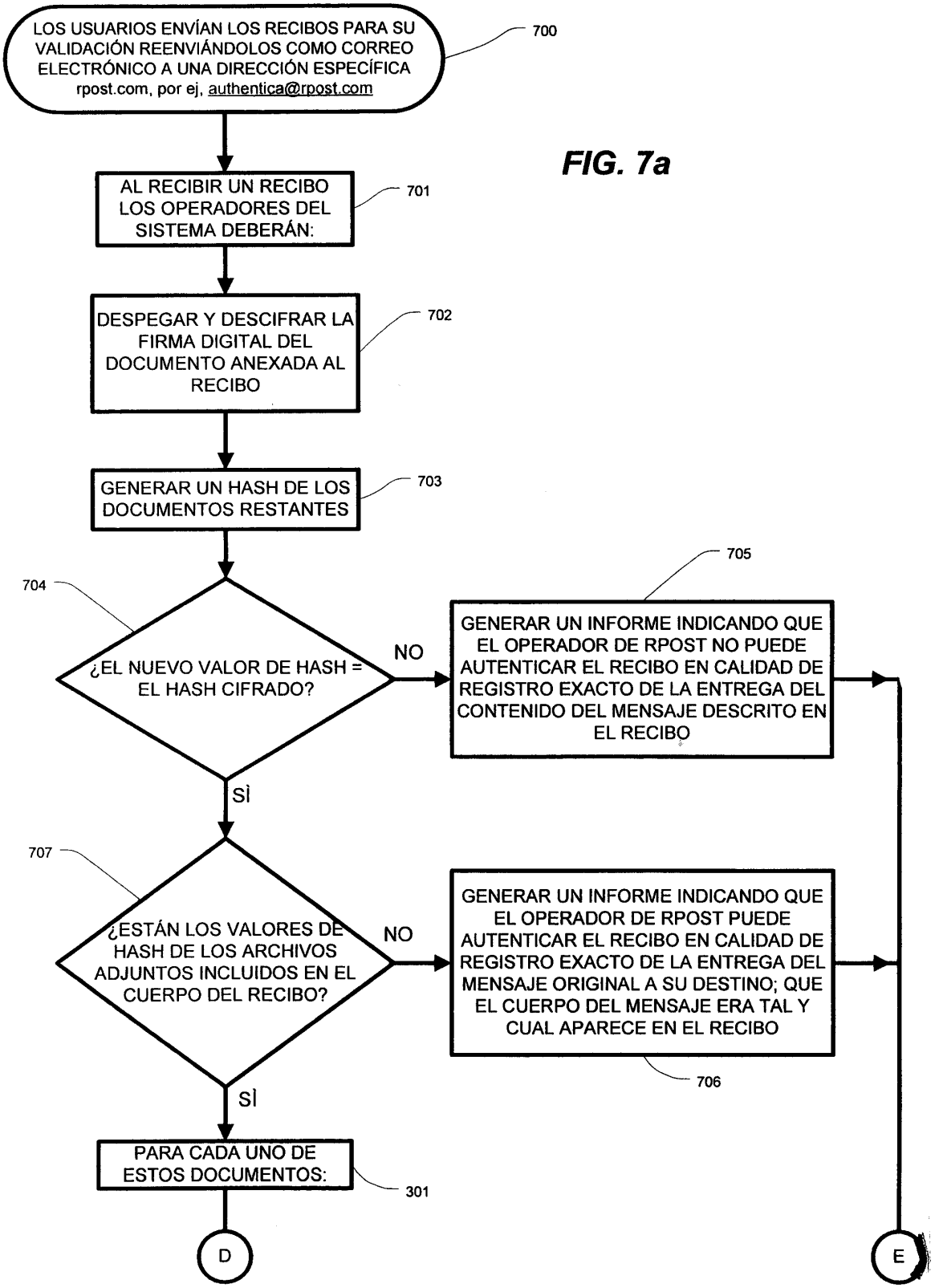

LOS USUARIOS ENVÍAN LOS RECIBOS PARA SU VALIDACIÓN REENVIÁNDOLOS COMO CORREO ELECTRÓNICO A UNA DIRECCIÓN ESPECÍFICA rpost.com, por ej, authentica@rpost.com
700
AL RECIBIR UN RECIBO LOS OPERADORES DEL SISTEMA DEBERÁN:
701
DESPEGAR Y DESCIFRAR LA FIRMA DIGITAL DEL DOCUMENTO ANEXADA AL RECIBO
702
GENERAR UN HASH DE LOS DOCUMENTOS RESTANTES
703
704
¿EL NUEVO VALOR DE HASH = EL HASH CIFRADO?
NO
705
GENERAR UN INFORME INDICANDO QUE EL OPERADOR DE RPOST NO PUEDE AUTENTICAR EL RECIBO EN CALIDAD DE REGISTRO EXACTO DE LA ENTREGA DEL CONTENIDO DEL MENSAJE DESCRITO EN EL RECIBO
SÌ
707
¿ESTÁN LOS VALORES DE HASH DE LOS ARCHIVOS ADJUNTOS INCLUIDOS EN EL CUERPO DEL RECIBO?
NO
GENERAR UN INFORME INDICANDO QUE EL OPERADOR DE RPOST PUEDE AUTENTICAR EL RECIBO EN CALIDAD DE REGISTRO EXACTO DE LA ENTREGA DEL MENSAJE ORIGINAL A SU DESTINO; QUE EL CUERPO DEL MENSAJE ERA TAL Y CUAL APARECE EN EL RECIBO
706
SÌ
PARA CADA UNO DE ESTOS DOCUMENTOS:
301
D
E

FIG. 7a

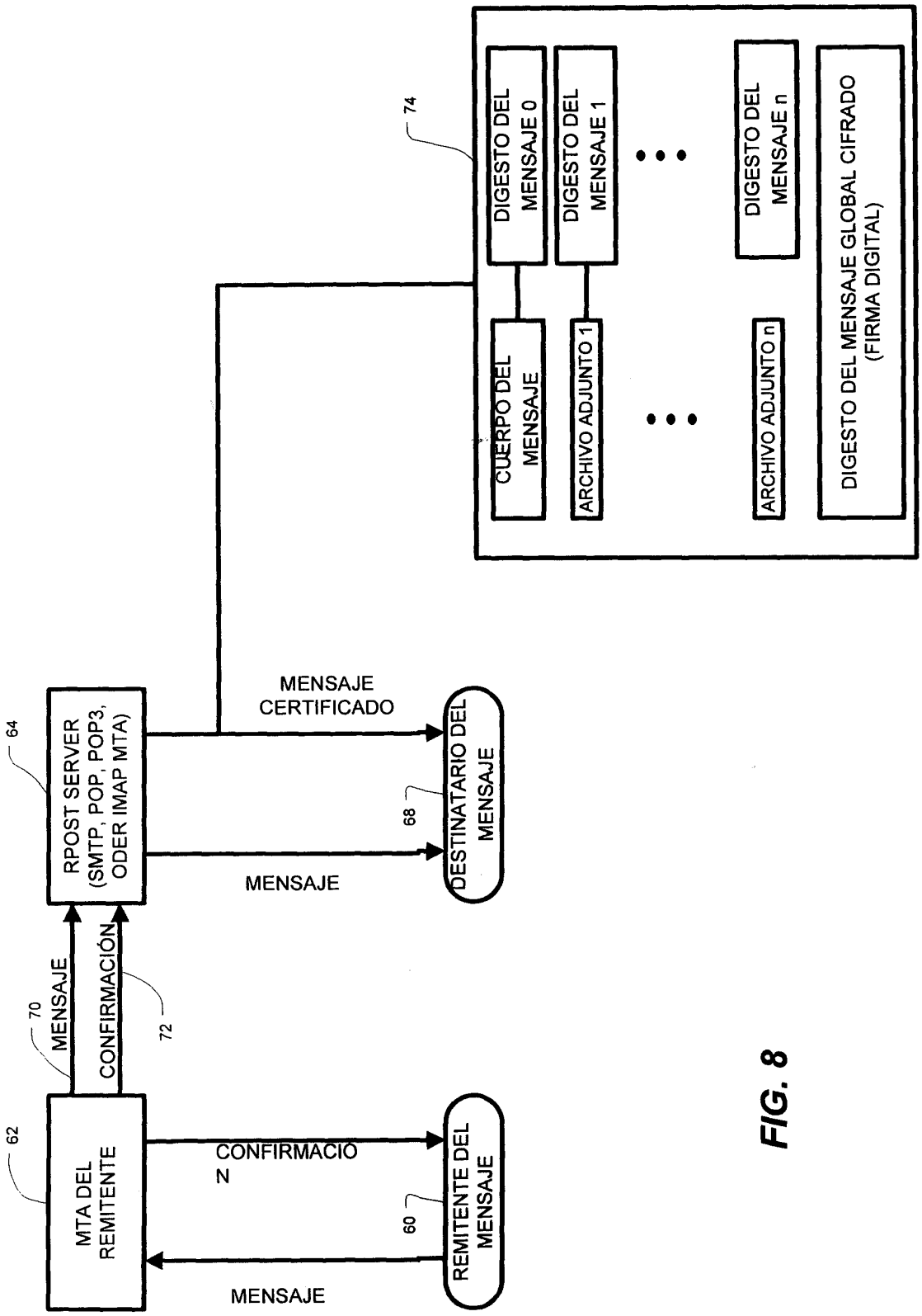
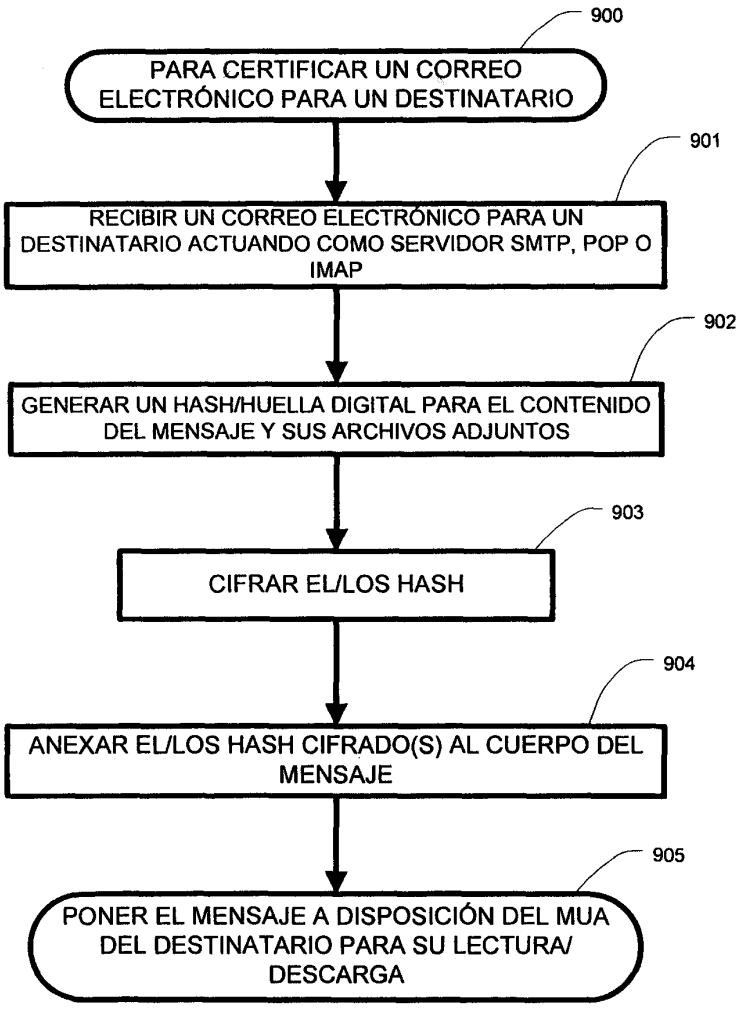

62
MTA DEL REMITENTE
64
RPOST SERVER (SMTP, POP, POP3, ODER IMAP MTA)
70
MENSAJE
CONFIRMACIÓN
72
MENSAJE CERTIFICADO
MENSAJE
68
DESTINATARIO DEL MENSAJE
CONFIRMACIÓN
MENSAJE
60
REMITENTE DEL MENSAJE
74
DIGESTO DEL MENSAJE 0
DIGESTO DEL MENSAJE 1
DIGESTO DEL MENSAJE n
CUERPO DEL MENSAJE
ARCHIVO ADJUNTO 1
ARCHIVO ADJUNTO n
DIGESTO DEL MENSAJE GLOBAL CIFRADO (FIRMA DIGITAL)

FIG. 8

FIG. 9


900
PARA CERTIFICAR UN CORREO ELECTRÓNICO PARA UN DESTINATARIO
901
RECIBIR UN CORREO ELECTRÓNICO PARA UN DESTINATARIO ACTUANDO COMO SERVIDOR SMTP, POP O IMAP
902
GENERAR UN HASH/HUELLA DIGITAL PARA EL CONTENIDO DEL MENSAJE Y SUS ARCHIVOS ADJUNTOS
903
CIFRAR EL/LOS HASH
904
ANEXAR EL/LOS HASH CIFRADO(S) AL CUERPO DEL MENSAJE
905
PONER EL MENSAJE A DISPOSICIÓN DEL MUA DEL DESTINATARIO PARA SU LECTURA/ DESCARGA

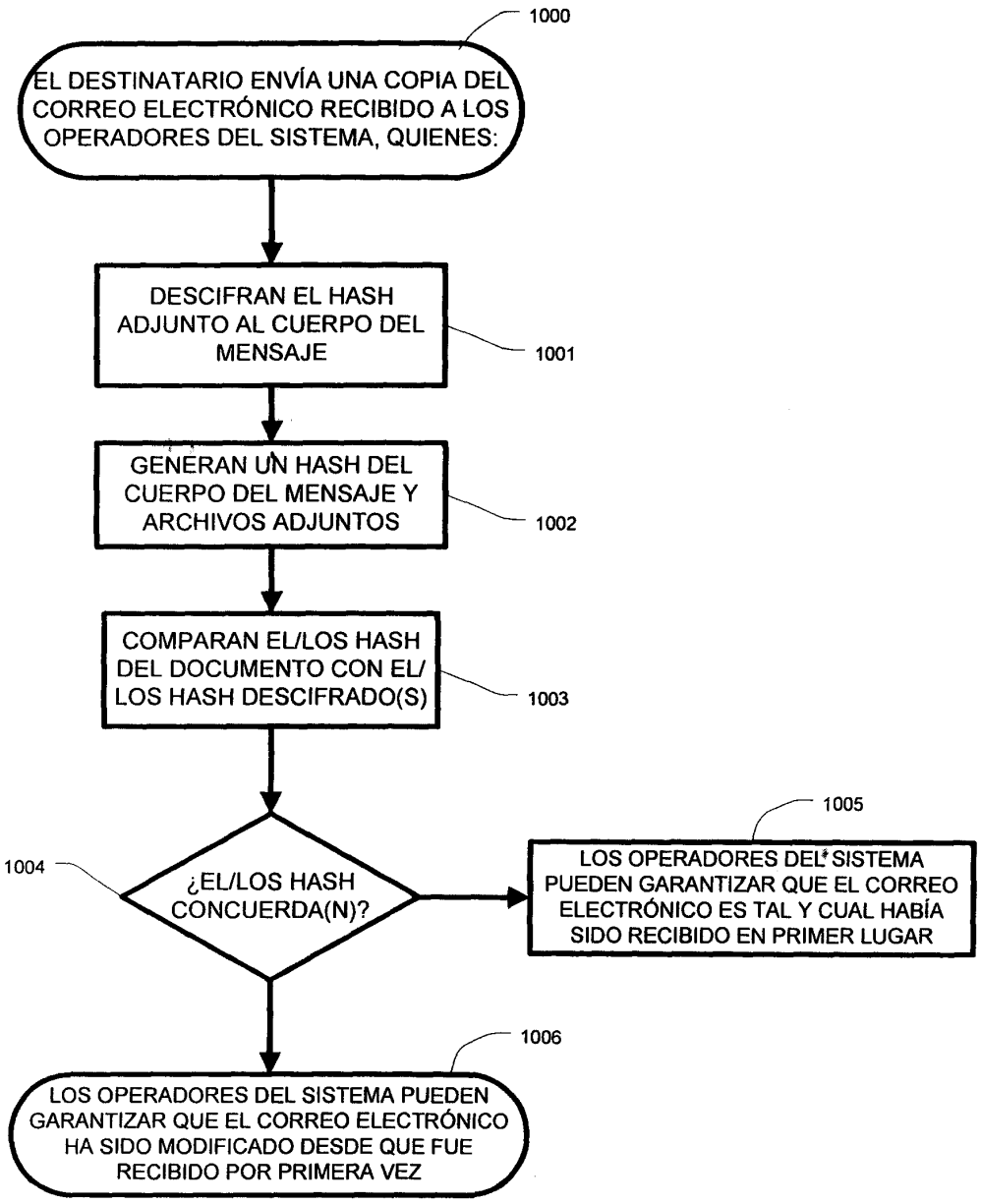

1000
EL DESTINATARIO ENVÍA UNA COPIA DEL CORREO ELECTRÓNICO RECIBIDO A LOS OPERADORES DEL SISTEMA, QUIENES:
DESCIFRAN EL HASH ADJUNTO AL CUERPO DEL MENSAJE
1001
GENERAN UN HASH DEL CUERPO DEL MENSAJE Y ARCHIVOS ADJUNTOS
1002
COMPARAN EL/LOS HASH DEL DOCUMENTO CON EL/ LOS HASH DESCIFRADO(S)
1003
1004
¿EL/LOS HASH CONCUERDA(N)?
1005
LOS OPERADORES DEL SISTEMA PUEDEN GARANTIZAR QUE EL CORREO ELECTRÓNICO ES TAL Y CUAL HABÍA SIDO RECIBIDO EN PRIMER LUGAR
1006
LOS OPERADORES DEL SISTEMA PUEDEN GARANTIZAR QUE EL CORREO ELECTRÓNICO HA SIDO MODIFICADO DESDE QUE FUE RECIBIDO POR PRIMERA VEZ

FIG. 10

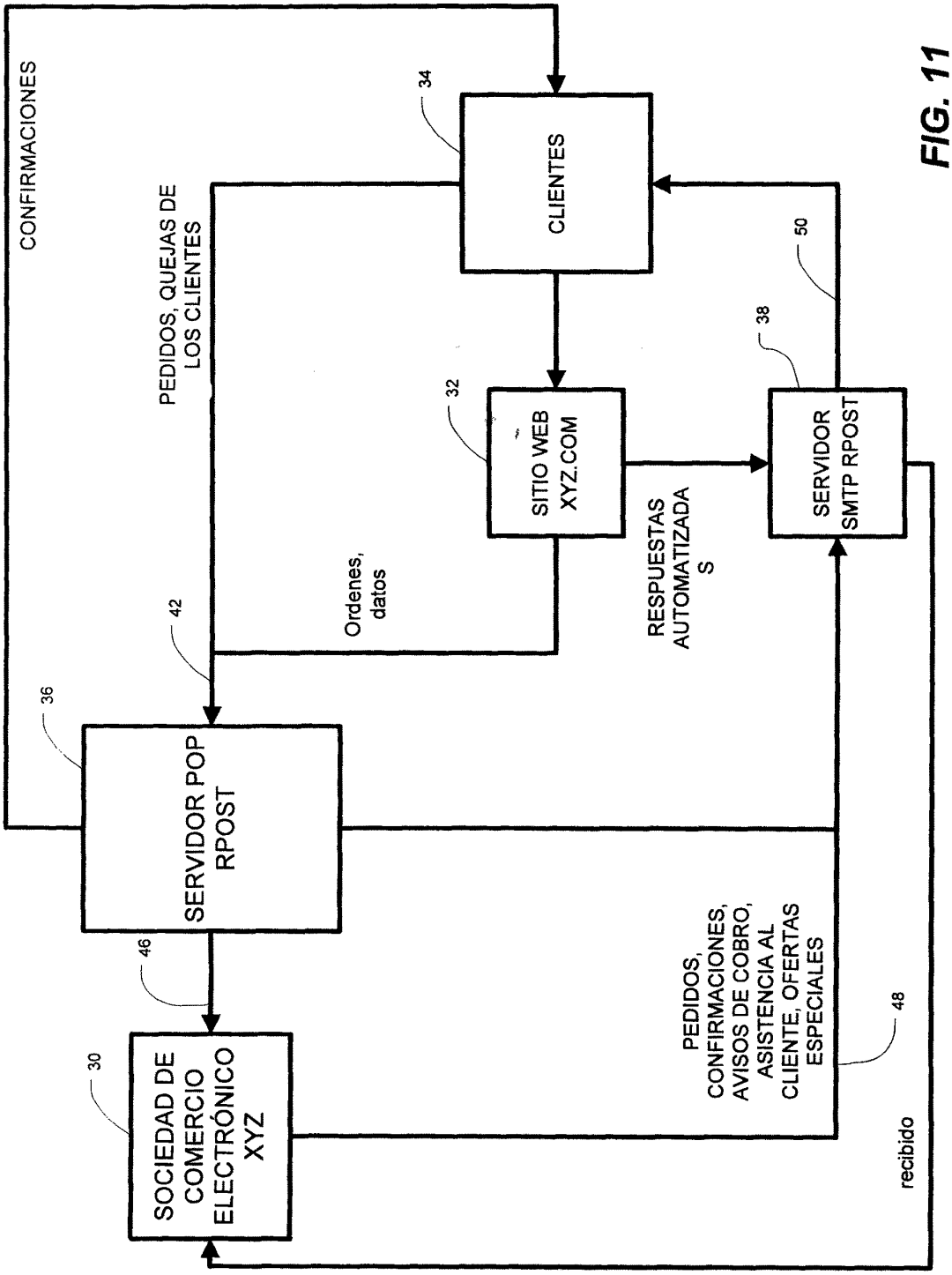

CONFIRMACIONES
34
CLIENTES
PEDIDOS, QUEJAS DE LOS CLIENTES
50
38
32
SITIO WEB XYZ.COM
SERVIDOR SMTP RPOST
Ordenes, datos
RESPUESTAS AUTOMATIZADAS
42
36
SERVIDOR POP RPOST
46
PEDIDOS, CONFIRMACIONES, AVISOS DE COBRO, ASISTENCIA AL CLIENTE, OFERTAS ESPECIALES
48
30
SOCIEDAD DE COMERCIO ELECTRÓNICO XYZ
recibido

FIG. 11

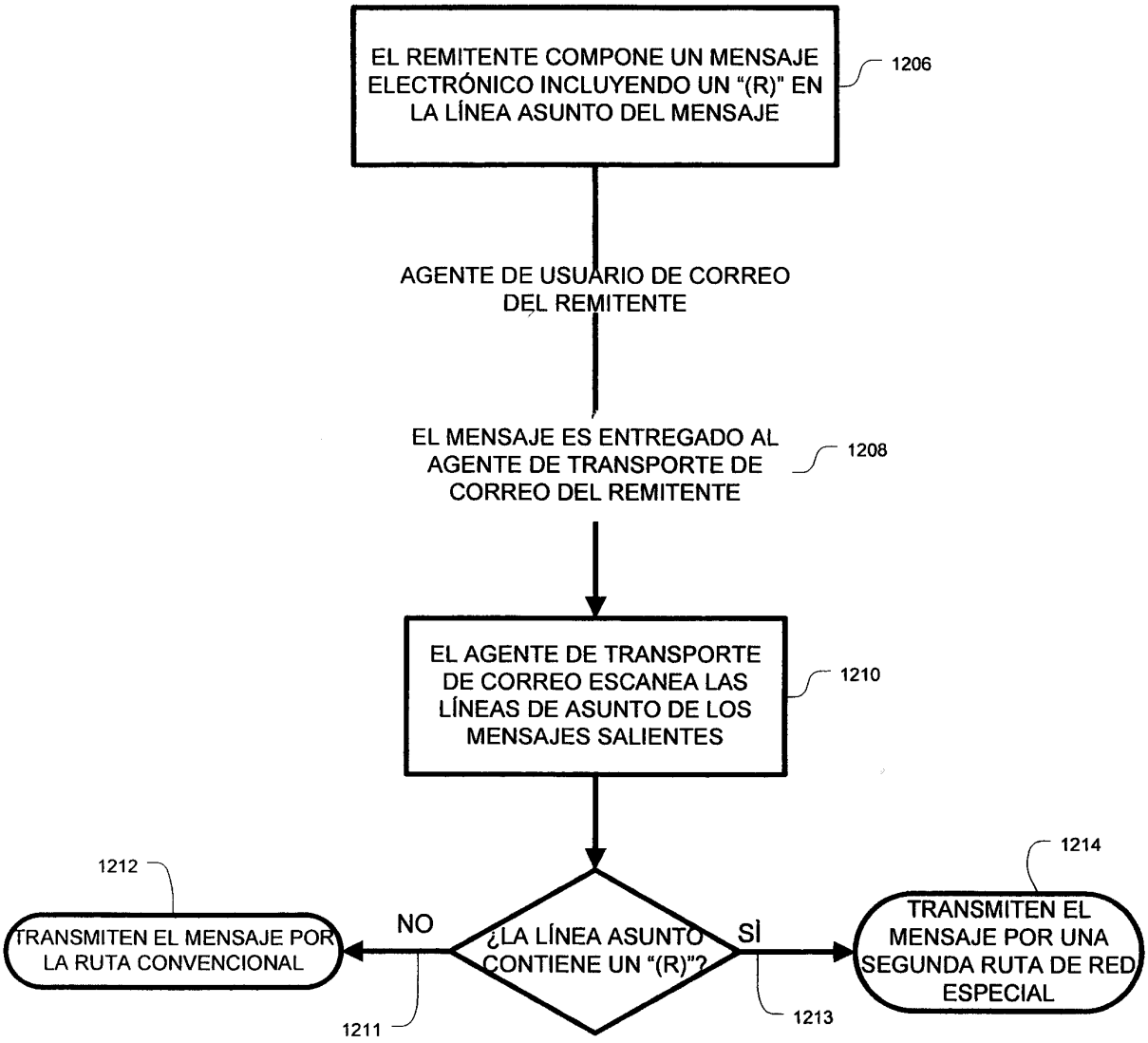

EL REMITENTE COMPONE UN MENSAJE ELECTRÓNICO INCLUYENDO UN "(R)" EN LA LÍNEA ASUNTO DEL MENSAJE
1206
AGENTE DE USUARIO DE CORREO DEL REMITENTE
EL MENSAJE ES ENTREGADO AL AGENTE DE TRANSPORTE DE CORREO DEL REMITENTE
1208
EL AGENTE DE TRANSPORTE DE CORREO ESCANEA LAS LÍNEAS DE ASUNTO DE LOS MENSAJES SALIENTES
1210
¿LA LÍNEA ASUNTO CONTIENE UN "(R)"?
NO
SÍ
1211
1212
TRANSMITEN EL MENSAJE POR LA RUTA CONVENCIONAL
1213
1214
TRANSMITEN EL MENSAJE POR UNA SEGUNDA RUTA DE RED ESPECIAL
Agente de Transporte de Correo del remitente

FIG. 12

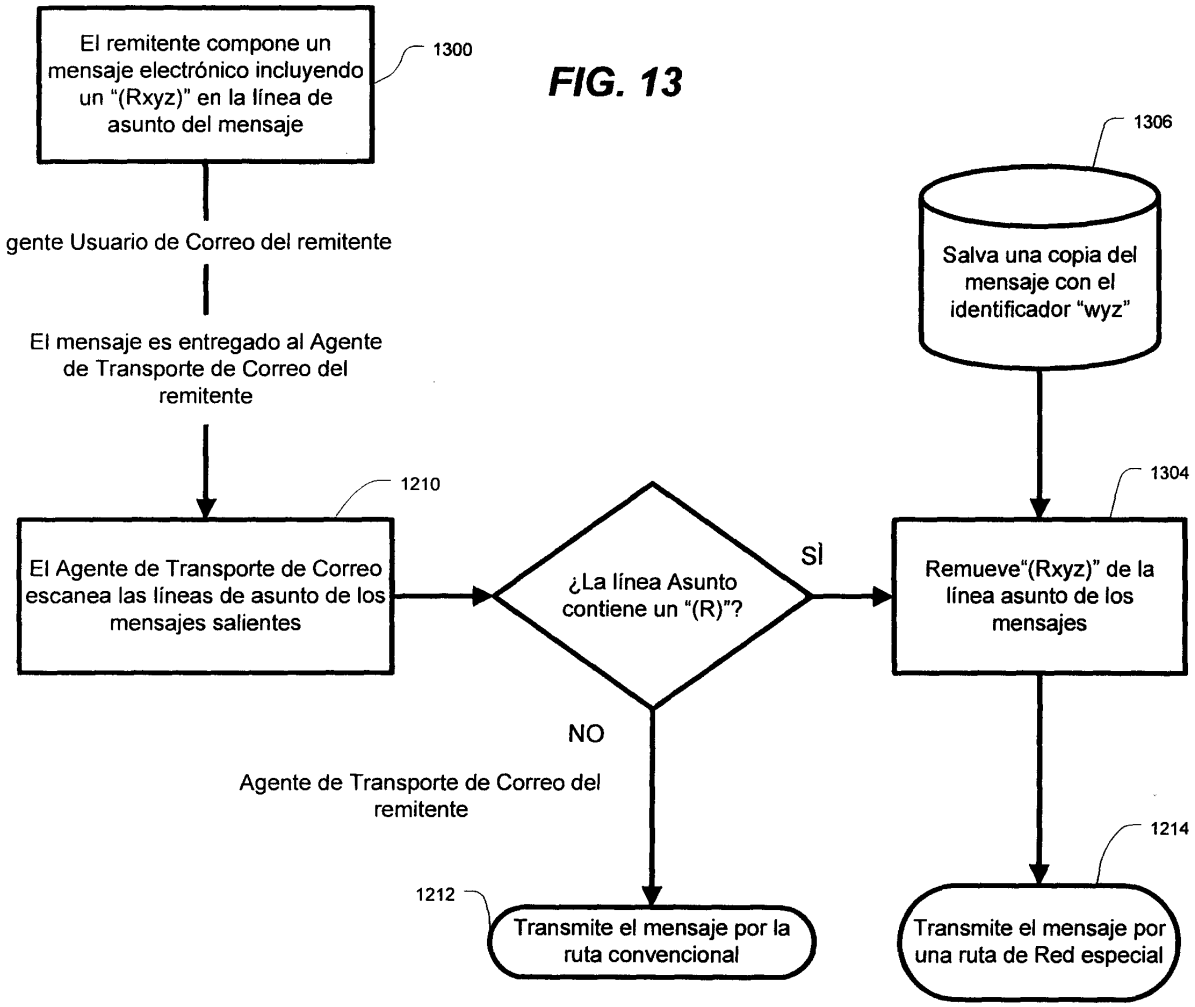

El remitente compone un mensaje electrónico incluyendo un "(Rxyz)" en la línea de asunto del mensaje
1300
gente Usuario de Correo del remitente
El mensaje es entregado al Agente de Transporte de Correo del remitente
1210
El Agente de Transporte de Correo escanea las líneas de asunto de los mensajes salientes
¿La línea Asunto contiene un "(R)"?
SÌ
NO
Agente de Transporte de Correo del remitente
1212
Transmite el mensaje por la ruta convencional
1306
Salva una copia del mensaje con el identificador "wyz"
1304
Remueve"(Rxyz)" de la línea asunto de los mensajes
1214
Transmite el mensaje por una ruta de Red especial

FIG. 13

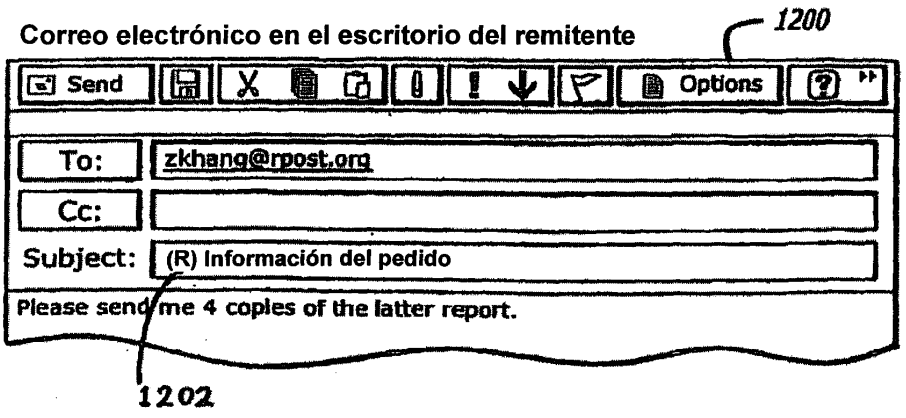

Correo electrónico en el escritorio del remitente
1200
Send
Options
To:
zkhang@rpost.org
Cc:
Subject:
(R) Información del pedido
Please send me 4 copies of the latter report.
1202

FIG. 14