(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 676 394**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.01.2012 PCT/EP2012/050583**

(87) Fecha y número de publicación internacional: **25.07.2013 WO13107499**

(96) Fecha de presentación y número de la solicitud europea: **16.01.2012 E 12708702 (1)**

(97) Fecha y número de publicación de la concesión europea: **04.04.2018 EP 2805455**

(54) Título: **Un procedimiento, un sistema y un producto de programa informático para certificar que un servidor de correo electrónico de destino ha recibido un mensaje de correo electrónico enviado por un emisor a al menos una dirección de destino**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.07.2018

(73) Titular/es:

TICÓ FARRÉ, CARLOS (100.0%)
C/ Dr. Roux 94 2 n. 1ª
08017 Barcelona, ES

(72) Inventor/es:

TICÓ FARRÉ, CARLOS

(74) Agente/Representante:

CONTRERAS PÉREZ, Yahel

DESCRIPCIÓN

UN PROCEDIMIENTO, UN SISTEMA Y UN PRODUCTO DE PROGRAMA INFORMÁTICO PARA CERTIFICAR QUE UN SERVIDOR DE CORREO ELECTRÓNICO DE DESTINO HA RECIBIDO UN MENSAJE DE CORREO ELECTRÓNICO ENVIADO POR UN EMISOR A AL MENOS UNA DIRECCIÓN DE DESTINO

La presente invención se refiere a un procedimiento de certificar que un mensaje de correo electrónico enviado por un emisor a través de un servidor de correo electrónico emisor a al menos una dirección de destino ha sido recibido por un servidor de correo electrónico de destino que gestiona la dirección de destino.

La invención también se refiere a un sistema y a un producto de programa informático adecuados para realizar dicho procedimiento.

TÉCNICA ANTERIOR

El correo electrónico (también conocido como e-mail) es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos. Este nombre se usa principalmente para describir el sistema que proporciona este servicio en Internet a través del protocolo para transferencia simple de correo (SMTP - *Simple Mail Transfer Protocol*), pero por extensión también se puede aplicar a sistemas similares que utilizan otras tecnologías. A través del correo electrónico no solo se puede enviar texto, sino todo tipo de documentos digitales. Su eficiencia, conveniencia y bajo coste hacen que el correo electrónico ocupe el lugar del correo normal para muchos usos comunes.

Se acepta ampliamente que en 1971 *Ray Tomlinson* se envió a sí mismo el primer correo electrónico de la historia a través de ARPANET, la red precursora de la Internet actual. Hoy en día, millones de personas y organizaciones de todo el mundo intercambian miles de millones de correos electrónicos todos los días. El correo electrónico es claramente uno de los procedimientos de comunicación más extendidos en el mundo, pero no es necesariamente eficiente como evidencia desde una perspectiva legal.

Los correos electrónicos se envían y reciben normalmente en formatos de texto plano o HTML y sin ningún tipo de firma; por lo tanto, tienen el mismo valor probatorio que cualquier otro documento privado que pueda presentarse como evidencia, por lo que es posible que los correos electrónicos deban ser corroborados por otros medios. Si se desea que un correo electrónico enviado sea constitutivo de prueba, es necesario acreditar este correo electrónico de alguna manera.

Hoy en día, existen muchos servicios en línea dirigidos a superar esta carencia a través de diferentes procedimientos, pero, a pesar de su fuerza legal, la mayoría de ellos comparten al menos uno de los siguientes inconvenientes: su coste; los correos electrónicos deben escribirse y/o enviarse desde un software cliente de correo electrónico no estándar; es posible que los destinatarios tengan que acceder a los correos electrónicos desde una fuente diferente al software cliente de correo electrónico estándar; y los destinatarios son conscientes de que los correos electrónicos y el acceso a su contenido están siendo registrados por deseo expreso de los emisores.

La solicitud europea EP1476995B1 divulga un procedimiento para transmitir un mensaje desde un emisor a una dirección de destino. En términos generales, un servidor recibe un mensaje de un emisor y transmite el mensaje a través de Internet a un destinatario. El servidor normalmente transmite el mensaje al destinatario por una primera ruta a través de Internet. Cuando el emisor indica en una posición particular del mensaje que el mensaje debe ser registrado, el servidor transmite el mensaje al destinatario por una segunda ruta a través de Internet. El emisor también puede proporcionar indicaciones adicionales en el mensaje para que el servidor procese el mensaje de otras formas especiales que normalmente el servidor no proporciona.

También se describe en el documento EP1476995B1 que después de conocer por medio del recibo o del agente del destinatario a través de Internet que el mensaje fue recibido con éxito, el servidor crea y envía al emisor un recibo electrónico. El recibo incluye al menos uno y preferiblemente todos de entre: el mensaje y archivos adjuntos, una tabla de entrega correcta/fallida que enumera las recepciones y los instantes de recepción del mensaje por parte de los agentes específicos del destinatario, y el fallo de otros agentes del destinatario en la recepción del mensaje y una firma digital del mensaje y archivos adjuntos posteriormente. Con la verificación de si la firma digital del recibo del emisor se corresponde 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 preciso.

Por lo tanto, el procedimiento descrito en el documento EP1476995B1 parece mantener buena evidencia en el tiempo sobre el contenido de un correo electrónico particular y su entrega a un destinatario, sin notificar al destinatario que el correo electrónico y el acceso a su contenido están siendo registrados. Por lo tanto, este procedimiento parece reducir la complejidad, el coste, la indiscreción y otros inconvenientes descritos anteriormente.

Sin embargo, el procedimiento del documento EP1476995B1 tiene el inconveniente de requerir adaptaciones específicas en el servidor de correo electrónico a través del cual se transmite el mensaje de correo electrónico desde el emisor a la dirección de destino. En efecto, dicho servidor de correo electrónico relacionado con el emisor debe tener implementadas las funcionalidades bajo las cuales se transmite el correo electrónico por una primera ruta o una segunda ruta, dependiendo de alguna indicación del emisor. Esto significa que si un emisor desea utilizar el procedimiento EP1476995B1 para enviar un correo electrónico, no podrá hacerlo a menos que las funcionalidades requeridas estén implementadas en su servidor de correo electrónico o en los servidores de su proveedor de correo electrónico. Dichas funcionalidades "extra" de redirigir el correo electrónico pueden disminuir innecesariamente la eficiencia del proceso general de envío del correo electrónico.

Además, incluso en el caso de que el servidor de correo electrónico emisor tenga implementadas las funcionalidades de redirigir el correo electrónico, puede haber situaciones en las que dicha redirección de correos electrónicos no se realice. Por ejemplo, si un usuario envía un mensaje de correo electrónico desde un dispositivo BlackBerry a través de la red de correo electrónico *Research In Motion Ltd.* (RIM), los servidores de correo electrónico RIM transmiten el mensaje de correo electrónico directamente al servidor de correo electrónico del destinatario. En dicho escenario, el mensaje de correo electrónico no es procesado por el servidor "normal" de correo electrónico del emisor. Por lo tanto, no se realiza la redirección del correo electrónico y, por lo tanto, cualquier indicación particular (solicitando, por ejemplo, el registro del correo electrónico) proporcionada por el emisor es insignificante e incomprensible para los servidores de correo electrónico RIM y no provoca que se realice un tratamiento especial del correo electrónico por parte de los servidores de correo electrónico RIM. En consecuencia, el correo electrónico no será registrado, como espera el emisor, y no se eliminará la indicación particular y seguirá siendo visible y observable para el destinatario.

El documento US2005198511 se refiere a un servidor que transmite un mensaje y archivos adjuntos desde un emisor a un destinatario. Se proporciona un hash del mensaje, una identificación del emisor y un hash de los archivos adjuntos para formar una cadena de datos. Se pueden incluir instrucciones para que el destinatario envíe un cifrado hash de la cadena a un sitio web en el servidor mediante correo electrónico registrado que proporciona unas opciones para obtener otras ventajas electrónicas.

El documento US2008/278740 divulga un procedimiento, un sistema y un producto de programa informático para la comunicación masiva de información a destinatarios a través de múltiples medios de entrega.

XP040139516: de *Victoria Bellotti et al.*, "*FLANNEL: Adding computation to electronic mail during transmission*", página 4, párrafo *IMPLEMENTATION* - página 5, párrafo *Routing*. Se refiere a nuevos sistemas de correo electrónico para dar soporte a la administración de tareas de correo electrónico.

RESUMEN DE LA INVENCIÓN

Es un objeto de la presente invención proporcionar un procedimiento que permita certificar que un mensaje de correo electrónico enviado por un emisor a través de un servidor de correo electrónico emisor a al menos una dirección de destino ha sido recibido por un servidor de correo electrónico de destino que gestiona la dirección de destino. Este objeto de la invención se logra de acuerdo con las reivindicaciones independientes. Otros aspectos de la invención se definen en las reivindicaciones dependientes. A lo largo de la descripción y las reivindicaciones, la palabra "comprender" y variaciones de la palabra no pretenden excluir otras características técnicas, aditivos, componentes o etapas. Objetos, ventajas y características adicionales de la invención serán evidentes para los expertos en la técnica al examinar la descripción o pueden aprenderse con la puesta en práctica de la invención. Los siguientes ejemplos y dibujos se proporcionan a modo de ilustración, y no se pretende que sean limitativos de la presente invención. Los signos de referencia relacionados con los dibujos y colocados entre paréntesis en una reivindicación, son únicamente para intentar aumentar la inteligibilidad de la reivindicación, y no deben interpretarse como una limitación del alcance de la reivindicación. Además, la presente invención cubre todas las posibles combinaciones de las formas de realización particulares y preferidas descritas en este documento.

DEFINICIONES

Para evitar confusiones y facilitar la comprensión de las descripciones relacionadas con la presente invención, esta sección proporciona numerosas y detalladas definiciones de conceptos clave en el contexto de la presente invención.

En el campo de la invención, el término "correo electrónico" (comúnmente conocido como e-mail) se refiere generalmente a un procedimiento de intercambio de mensajes digitales de un emisor a uno o más destinatarios, principalmente a través de Internet u otras Redes informáticas.

Un mensaje de correo electrónico consta de tres componentes: la envolvente (o sobre) del mensaje, el encabezado del mensaje y el cuerpo del mensaje.

La "envolvente del mensaje" contiene los parámetros de entrega comunicados por el SMTP en el proceso de transporte de mensajes de correo electrónico entre sistemas. A lo largo de esta solicitud de patente, el estándar SMTP, la transmisión SMTP, los datos SMTP, la confirmación de aceptación y la confirmación de entrega, se refieren a la envolvente (o sobre) del mensaje. Para otros fines, el mensaje de correo electrónico solo se referirá al encabezado del mensaje y al cuerpo del mensaje.

El "encabezado del mensaje" contiene información de control, que incluye, como mínimo, la dirección de correo electrónico de un emisor y una o más direcciones de destino. Por lo general, también se agrega información descriptiva como, por ejemplo, un campo de encabezado de asunto, direcciones IP de cualquier sistema a través del cual se ha transportado el correo electrónico o la fecha y hora locales en las que se envió el mensaje. Cada mensaje de correo electrónico tiene exactamente un encabezado, que está estructurado en campos. Cada campo tiene un nombre y un valor. La RFC 5322 especifica la sintaxis precisa de los encabezados de mensaje.

Con respecto a esta solicitud de patente, el "cuerpo del mensaje" se refiere específicamente a lo que realmente se imprimirá cuando se imprima un mensaje de correo electrónico desde cualquier software cliente de correo electrónico. Esto excluye el encabezado del mensaje y cualquier archivo eventualmente adjunto al mensaje de correo electrónico.

El término "certificación" se refiere a la capacidad de demostrar que un mensaje de correo electrónico particular, incluidos sus contenidos y archivos digitales eventualmente adjuntos, fue realmente entregado a un destinatario particular y cuando tuvo lugar dicha entrega.

El término "archivo de certificación" se refiere a un archivo PDF (o cualquier otro formato apropiado o equivalente) que recopila información de un mensaje de correo electrónico particular, es decir de su sobre (o envolvente), encabezado y cuerpo, los nombres de todos los archivos digitales eventualmente adjuntos a ese mensaje de correo electrónico o de todos los archivos digitales relacionados o generados como parte del procedimiento con respecto a la certificación de ese mensaje en particular, y el valor hash de cualquiera de estos archivos digitales.

Para fines legales y según se detalla a lo largo de esta solicitud de patente, este archivo de certificación PDF finalmente es firmado digitalmente y con una marca (o sello) de tiempo para otorgar la integridad de los datos contenidos en el mismo, establecer de manera confiable la fecha en la que fue creado y, finalmente, habilitarlo para comparar la información contenida en el mismo con los datos originales a partir de los cuales se obtuvo esta información y probar la integridad de estos datos originales.

El término "huella digital electrónica" se refiere al valor hash, también conocido como el resumen del mensaje o simplemente resumen, que se obtiene por medio de una función hash criptográfica a partir de un bloque de datos, también conocido como el mensaje. Con respecto a esta solicitud de patente, el bloque de datos puede ser un mensaje de correo electrónico, un archivo digital eventualmente adjunto al mensaje de correo electrónico o cualquier archivo digital relacionado o generado como parte del procedimiento con respecto a un evento de certificación particular.

El término "identificador único" se refiere a una clave de identificación en forma de cadena alfanumérica que identifica exclusivamente un evento particular, concretamente un evento de certificación como resultado de la aplicación del procedimiento, y que por esta razón debe ser único y diferente de cualquier otro identificador. Con respecto a esta solicitud de patente, el identificador único comprende no solo el evento, sino también todos los datos y archivos obtenidos o generados a partir de ese evento en particular.

Finalmente, el término "servidor de correo electrónico" se refiere al software que transfiere mensajes de correo electrónico desde un sistema informático a otro usando una arquitectura de aplicación cliente-servidor, concretamente un Agente de Transferencia de Mensajes o Agente de Transferencia de Correos (MTA – *Mail Transfer Agent*). Un MTA implementa ambas partes de cliente (envío) y de servidor (recepción) del protocolo para transferencia simple de correo (SMTP), por lo que es capaz de enviar y recibir mensajes de correo electrónico. También se refiere a dispositivos electrónicos (por ejemplo, ordenadores informáticos o terminales móviles - teléfonos inteligentes, tabletas, etc.) que realizan la función de MTA.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación se describirán formas de realización particulares de la presente invención a modo de ejemplos no limitativos, con referencia a los dibujos adjuntos, en los que:

La Figura 1 es una representación esquemática de una configuración de sistemas que comprende un servidor de certificación de correos según formas de realización de la invención;

La figura 2 muestra el contenido de un archivo PDF que comprende datos que evidencian que se ha aceptado un mensaje de correo electrónico en el destino, según formas de realización de la invención; y

La figura 3 muestra el contenido del archivo PDF que comprende datos que representan el cuerpo y el encabezado del mensaje de correo electrónico al que se refiere la figura 2, según formas de realización de la invención.

DESCRIPCIÓN DETALLADA DE FORMAS DE REALIZACIÓN DE LA INVENCIÓN

En las siguientes descripciones, se exponen numerosos detalles específicos para proporcionar una comprensión completa de la presente invención. Un experto en la materia entenderá, sin embargo, que la presente invención puede ponerse en práctica sin algunos o todos estos detalles específicos. En otros casos, no se han descrito en detalle elementos bien conocidos con el fin de no dificultar innecesariamente la descripción de la presente invención.

La Figura 1 representa esquemáticamente una configuración general de sistemas que es adecuada para realizar formas de realización del procedimiento de la invención. En particular, se puede enviar un mensaje de correo electrónico desde un emisor 101 a través de un servidor de correo electrónico emisor 102 a una o más direcciones de destino indicadas en el encabezado del mensaje de correo electrónico. Cada una de dichas direcciones de destino puede ser gestionada por un servidor de correo electrónico de destino 106 diferente y puede representar al menos un destinatario 107 del mensaje de correo electrónico. La figura 1 solo muestra un destinatario 107 y un servidor de correo electrónico de destino 106 relacionado por razones de simplicidad, pero debe entenderse que formas de realización del procedimiento pueden soportar varias direcciones de destino que se refieren a varios destinatarios gestionados por varios servidores de correo electrónico de destino.

El servidor de correo electrónico emisor 102 y el servidor de correo electrónico de destino 106 están conectados a través de al menos una red de comunicaciones 103, 105 tal como, por ejemplo, Internet. La figura 1 muestra una primera red 103 y una segunda red 105, pero dichas dos redes 103, 105 pueden ser la misma red de comunicaciones.

Un mensaje de correo electrónico "normal" procedente del emisor 101 generalmente comprenderá, en el campo del encabezado que se refiere a la dirección de destino, la dirección de destino para el destinatario 107. Por ejemplo, el campo que se refiere a la dirección de destino puede comprender "recipiente@destino.com" como la dirección de destino que representa al destinatario 107. Siguiendo el protocolo estándar para la transmisión de correos electrónicos del protocolo para transferencia simple de correo (SMTP), el servidor de correo electrónico emisor 102 se conectará con el servidor de correo electrónico de destino 106 resolviendo el registro de intercambio de correos (MX) para el nombre de dominio "destino.com", a fin de transmitir el correo electrónico.

Un registro de intercambio de correos (registro MX) es un tipo de registro de recursos en el sistema de nombres de dominio (DNS) que especifica la dirección IP de un servidor de correo responsable de aceptar mensajes de correo electrónico dirigidos a un nombre de dominio determinado, y un valor de preferencia utilizado para priorizar la entrega de correos si se especifican varios servidores de correo (en realidad, registros MX). El conjunto de registros MX de un nombre de dominio especifica cómo se debe encaminar el correo electrónico de acuerdo con el estándar SMTP.

El Sistema de Nombres de Dominio (DNS) es un sistema jerárquico de nombres distribuidos para sistemas informáticos, servicios o cualquier recurso conectado a Internet o a una red privada. El DNS asocia información diferente con nombres de dominio asignados a cada una de las entidades participantes. Lo que es más importante, el DNS traduce nombres de dominio que son significativos para los humanos en identificadores numéricos asociados con equipos de red con el fin de localizar y direccionar estos dispositivos en todo el mundo.

En el contexto de la presente invención, el mensaje de correo electrónico (a certificar) procedente del emisor 101 puede comprender, en el campo que se refiere a la dirección de destino, el resultado de concatenar una primera sub-cadena que representa la dirección de destino final y real que representa el destinatario 107 y una segunda sub-cadena que representa un nombre de dominio adicional (precedido por un punto). Los registros DNS de este nombre de dominio adicional se pueden haber configurado para aceptar comodines para los registros MX de ese nombre de dominio adicional y devolver siempre la misma ruta al servidor de correo electrónico de certificación 104 independientemente de lo que contenga el comodín. Por ejemplo, el campo del encabezado que se refiere a la dirección de destino puede contener la siguiente cadena: "recipiente@destino.com.eevid.com", que es el resultado de concatenar una primera cadena "recipiente@destino.com" (dirección de destino real) y una segunda sub-cadena "eevid.com" (nombre de dominio adicional) precedida por un punto.

Según lo definido por la RFC 1034 de 1987, "*Domain names - Concepts and facilities*" (Nombres de dominio - Conceptos y servicios), y aclarado en 2006 en la RFC 4592, "*The Role of Wildcards in the Domain Name System*" (El papel de los comodines en el sistema de nombres de dominio), los registros comodín ofrecerán la capacidad de mapear todos (o una parte) de los registros de un nombre de dominio determinado con una IP. Un registro DNS

comodín se especifica utilizando un "*" como la etiqueta (parte) de más a la izquierda de un nombre de dominio, por ejemplo: “*. eevid.com”.

Es importante tener en cuenta que una respuesta de enrutamiento de un registro MX basado en un DNS comodín es indistinguible de la de un registro MX basado en un DNS no comodín; sin importar si los registros MX de nombre de dominio se basan en una configuración DNS comodín o no, un servidor de correo electrónico que intente entregar un mensaje de correo electrónico a ese nombre de dominio en particular se comportará exactamente de la misma manera.

Por lo tanto, el servidor de correo electrónico emisor 102 normalmente envía el mensaje de correo electrónico a este servidor de correo electrónico de certificación 104 de acuerdo con los registros MX de nombre de dominio que apuntan al servidor de correo electrónico de certificación 104. Una vez que el servidor de correo electrónico de certificación 104 ha recibido el mensaje de correo electrónico, este servidor de correo electrónico de certificación 104 puede estar listo para generar un archivo de certificación relacionado con el mensaje de correo electrónico.

El procedimiento puede comprender validar la dirección de correo electrónico emisora 101, y verificar que dicha dirección de correo electrónico corresponde a un emisor registrado 101. Si la dirección de correo electrónico emisora 101 está registrada, el servidor de correo electrónico de certificación 104 puede realizar la generación del archivo de certificación. Si la dirección de correo electrónico emisora 101 no está registrada, la solicitud de certificación del emisor 101 puede ser rechazada y, por lo tanto, por ejemplo, puede no generarse el archivo de certificación.

El servidor de correo electrónico de certificación 104 puede generar un identificador único para ser utilizado como una referencia interna del evento de certificación asociado con ese mensaje de correo electrónico particular y para cualquier dato generado a partir del mismo y de su entrega por medio de formas de realización del procedimiento de certificación. Dicho identificador único del evento de certificación puede tener la forma de cadena alfanumérica y se puede almacenar en un repositorio de datos de certificación.

Entonces, el servidor de correo electrónico de certificación 104 puede extraer datos del encabezado del mensaje de correo electrónico que pueden ser relevantes con respecto al mensaje de correo electrónico como, por ejemplo, la dirección IP de la que proviene el mensaje, la dirección de correo electrónico emisora 101, las direcciones de destino de los destinatarios previstos 107, el asunto del mensaje de correo electrónico, etc. Por ejemplo, el servidor de correo electrónico de certificación 104 puede obtener la dirección de destino real (por ejemplo, de acuerdo con el ejemplo propuesto anteriormente: "recipiente@destino.com") del campo de encabezado que se refiere a la dirección de destino del mensaje de correo electrónico. La dirección de destino real se puede obtener, por ejemplo, detectando y eliminando posteriormente del encabezado del mensaje la cadena ".eevid.com", que corresponde al nombre de dominio adicional que apunta al servidor de correo electrónico de certificación 104. Estos datos extraídos del encabezado del correo electrónico se pueden almacenar en un repositorio como, por ejemplo, el repositorio de datos de certificación.

Una vez que el servidor de correo electrónico de certificación 104 ha obtenido la dirección de destino, el servidor de correo electrónico de certificación 104 puede iniciar la entrega del mensaje de correo electrónico a la dirección de destino 107 resolviendo normalmente los registros MX para el nombre de dominio "destino.com", que encaminará el mensaje de correo electrónico hacia el servidor de correo electrónico de destino 106. Una vez que se recupera un registro MX válido, es decir, una dirección IP válida, el servidor de correo electrónico 104 puede asumir que un servidor de correo electrónico 106 detrás de esa dirección IP aceptará o rechazará mensajes de correo electrónico para el nombre de dominio “destino.com” y, en consecuencia, el servidor de correo electrónico de certificación 104 puede intentar la entrega del mensaje de correo iniciando una transmisión SMTP con el servidor de correo electrónico de destino 106. Cuando tiene éxito y durante dicha transmisión SMTP, el servidor de correo electrónico de certificación 104 puede recibir del servidor de correo electrónico de destino 106 una confirmación de la aceptación o rechazo del mensaje de correo electrónico en forma de, por ejemplo, un código "250 OK", siguiendo las recomendaciones del SMTP. Esta confirmación de aceptación o rechazo se puede almacenar en un repositorio como, por ejemplo, el repositorio de datos de certificación.

El servidor de correo electrónico de destino 106 puede proporcionar, por ejemplo, datos relativos al mensaje de correo electrónico, su destinatario o la aceptación/rechazo del mensaje de correo electrónico que incluye, pero no se limita a, un identificador de destino del mensaje de correo electrónico que generalmente representa un identificador único e interno, mediante el cual el servidor de correo electrónico de destino 106 ha registrado tanto el mensaje de correo electrónico como todos los eventos y hechos relacionados con su transmisión. Estos datos proporcionados por el servidor de correo electrónico de destino 106 pueden almacenarse en un repositorio tal como, por ejemplo, el repositorio de datos de certificación.

El servidor de correo electrónico de certificación 104 puede generar un registro que comprende datos que representan al menos la confirmación de la aceptación/rechazo del mensaje de correo electrónico y otros datos

relacionados tales como, por ejemplo, el identificador de destino del mensaje de correo electrónico. Después de eso, el servidor de correo electrónico de certificación 104 puede enviar el registro al emisor 101 a través del servidor de correo electrónico emisor 102. Este registro de datos puede obtenerse, por ejemplo, del repositorio de datos de certificación. Alternativamente a o además de enviar el registro al emisor 101, el servidor de correo electrónico de certificación 104 puede enviar el registro a la dirección de destino a través del servidor de correo electrónico de destino 106.

Alternativamente a o además de enviar el registro al emisor 101, la certificación puede no enviar el registro al emisor 101 sino a una dirección de destino relacionada con el emisor 101. Por ejemplo, para una pluralidad de emisores 101 que pertenecen a la misma empresa, se puede enviar el registro a una única dirección de destino de la empresa en lugar de enviar el registro a cada emisor 101 de la empresa.

En algunas formas de realización, el servidor de correo electrónico de certificación 104 puede almacenar en un repositorio (como, por ejemplo, el repositorio de datos de certificación) datos que representan la comunicación entre el servidor de correo electrónico emisor 102 y el servidor de correo electrónico de certificación 104 y entre el servidor de correo electrónico de certificación 104 y el servidor de correo electrónico de destino 106. Dichos datos pueden incluir, por ejemplo, las direcciones IP para cada servidor de correo electrónico, y/o el nombre de host de cada servidor de correo, y/o la confirmación de aceptación/rechazo del mensaje de correo electrónico por parte del servidor de correo electrónico de destino 106, etc. Dicho registro de datos puede comprender además datos que representan la comunicación entre el servidor de correo electrónico de certificación 104 y el servidor de correo electrónico de destino 106.

En formas de realización de la invención, el procedimiento puede comprender obtener una huella digital del mensaje de correo electrónico, que se puede almacenar en un repositorio tal como, por ejemplo, el repositorio de datos de certificación.

La huella digital del mensaje de correo electrónico puede comprender un valor hash que representa el mensaje de correo electrónico. Este valor hash se puede obtener aplicando una función hash criptográfica a una versión consistente del mensaje de correo electrónico. La expresión "versión consistente" se refiere a un formato del mensaje de correo electrónico que siempre produce el mismo valor hash al aplicar la misma función hash criptográfica. Por ejemplo, cuando un correo electrónico original es reenviado como un archivo adjunto a otro correo electrónico, la aplicación de la función hash criptográfica al mensaje de correo electrónico original y al correo electrónico adjunto puede generar diferentes valores hash. Por lo tanto, se puede entender que el formato de correo electrónico puede generar "versiones inconsistentes" del mensaje de correo electrónico.

Una función hash criptográfica es un procedimiento determinista que toma un bloque arbitrario de datos y devuelve una cadena de bits de tamaño fijo, el valor hash (criptográfico), de modo que un cambio accidental o intencionado en los datos cambiará el valor hash. Los datos a codificar (es decir, proporcionados a la función hash) a menudo se denominan "mensaje" y el valor hash (es decir, el resultado de la función hash aplicada al "mensaje") normalmente se denomina resumen del mensaje o simplemente resumen.

Se puede obtener una "versión consistente" del mensaje de correo electrónico, por ejemplo, generando un archivo PDF a partir del mensaje de correo electrónico. El PDF (*Portable Document Format* – formato de documento portátil) es un estándar abierto para el intercambio de documentos. Este formato de archivo, creado por *Adobe Systems* en 1993, se utiliza para representar documentos de una manera independiente del software de aplicación, hardware y sistemas operativos. Por lo tanto, se entiende que diferentes ejecuciones de la misma función hash criptográfica en un PDF que representa el mismo mensaje de correo electrónico producen el mismo valor hash. Este archivo PDF obtenido a partir del mensaje de correo electrónico se puede almacenar en un repositorio como, por ejemplo, el repositorio de datos de certificación.

Por lo tanto, la obtención de la huella digital del mensaje de correo electrónico puede comprender la aplicación de una función hash criptográfica a un archivo PDF generado a partir del mensaje de correo electrónico. Este archivo PDF se puede obtener, por ejemplo, imprimiendo el mensaje de correo electrónico a una impresora virtual PDF. Esta huella digital del mensaje de correo electrónico (por ejemplo, valor hash) y los datos relacionados se pueden almacenar en un repositorio como, por ejemplo, el repositorio de datos de certificación.

En formas de realización preferidas, cuando el mensaje de correo electrónico comprende al menos un archivo adjunto, el procedimiento puede comprender además obtener una huella digital de cada archivo adjunto. Dicha huella digital de cada archivo adjunto se puede generar aplicando una función hash criptográfica al archivo adjunto. Estas huellas digitales de archivos adjuntos (por ejemplo, valores hash) y datos relacionados se pueden almacenar en un repositorio como, por ejemplo, el repositorio de datos de certificación.

Una función hash que se puede usar es la SHA-256 que pertenece al conjunto de funciones hash criptográficas del estándar SHA-2, aunque se puede usar otra función hash si, por ejemplo, se demuestra en el futuro que la SHA-256 no es lo suficientemente segura. Por ejemplo, las funciones SHA-1 y MD5 fueron consideradas inicialmente en el contexto de esta invención, pero finalmente se descartaron debido a algunos fallos de seguridad reportados. La seguridad de una función hash está determinada por su resistencia a las colisiones. Una función hash es resistente a las colisiones si su aplicación a diferentes mensajes (datos a codificar) produce un resumen de mensaje diferente. Aunque la SHA-256 se utiliza actualmente en el contexto de esta invención, podría sustituirse en el futuro por otra función hash con una resistencia a las colisiones mejorada (es decir, más segura) tal como, por ejemplo, la SHA-3, que es un nuevo estándar hash actualmente en desarrollo en el momento de esta solicitud de patente.

En formas de realización del procedimiento, el servidor de correo electrónico de certificación 104 puede generar un archivo de certificación que comprenda al menos la huella digital del mensaje de correo electrónico y la confirmación de aceptación o rechazo del mensaje de correo electrónico procedente del servidor de correo electrónico de destino. Este archivo de certificación puede comprender además otros datos relacionados con el mensaje de correo electrónico, su contenido y su entrega al servidor de correo electrónico 106; estos otros datos pueden comprender, por ejemplo, el identificador único del evento de certificación y/o datos relevantes extraídos del encabezado del mensaje de correo electrónico, y/o el nombre de archivo de cada uno de los archivos adjuntos al mensaje de correo electrónico, y/o el nombre del archivo PDF de la versión consistente del mensaje de correo electrónico, y/o los valores hash obtenidos de cada archivo relacionado con el mensaje de correo electrónico y/o archivos adjuntos, y/o el nombre de host del servidor de correo electrónico emisor desde el cual se recibe el mensaje de correo electrónico, y/o los datos SMTP registrados tras la entrega del mensaje de correo electrónico al servidor de correo electrónico 106. Todos los datos incluidos en el archivo de certificación se pueden obtener de un repositorio en el que dichos datos pueden haber sido almacenados tal como, por ejemplo, el repositorio de datos de certificación. Este archivo de certificación puede ser, por ejemplo, un archivo PDF.

En formas de realización del procedimiento, el servidor de correo electrónico de certificación 104 puede firmar digitalmente el archivo de certificación. Dicha firma digital se puede considerar una buena forma de garantizar la integridad del contenido del archivo de certificación. Esta firma digital y datos relacionados se pueden almacenar en un repositorio como, por ejemplo, el repositorio de datos de certificación.

En algunas formas de realización, la firma digital puede incluir una credencial (*token*) de marca de tiempo que establecerá indudablemente la fecha precisa en la que se firmó digitalmente el archivo de certificación. Esta marca de tiempo puede ser proporcionada por una Autoridad de Sellado de Tiempo (TSA – *Time Stamping Authority*) independiente que cumpla con la RFC 3161. Esta credencial de marca (o sello) de tiempo y datos relacionados se pueden almacenar en un repositorio como, por ejemplo, el repositorio de datos de certificación.

De acuerdo con el estándar RFC 3161, una marca (o sello) de tiempo confiable es una marca de tiempo emitida por un tercero de confianza (TTP – *trusted third party*) que actúa como una Autoridad de Sellado de Tiempo (TSA). Se usa para demostrar la existencia de ciertos datos antes de cierto punto (por ejemplo, contratos, datos de investigación, registros médicos, etc.) sin la posibilidad de que el propietario pueda antedatar (o poner una fecha anterior en) las marcas de tiempo. Se pueden usar múltiples TSA para aumentar la confiabilidad y reducir la vulnerabilidad.

Debido al hecho de que las firmas digitales se basan en algoritmos criptográficos que se pueden romper en el futuro, la firma digital de un archivo firmado digitalmente se considerará válida durante un período de tiempo limitado, después del cual la firma caducará (o dejará de estar vigente). Este período de tiempo es normalmente de algunos años. Para mantener en vigencia la firma digital del archivo de certificación, algunas formas de realización del procedimiento pueden comprender el firmado (o firma) digital periódico del archivo de certificación y el sellado de tiempo de la firma digital. Esta firma y sellado de tiempo periódicos se pueden generar, por ejemplo, un tiempo razonablemente corto antes del vencimiento de la firma actual y del sello de tiempo relacionado.

En formas de realización del procedimiento, la firma digital del archivo de certificación se puede generar aplicando PAdES (*PDF Advanced Electronic Signatures* – firmas electrónicas avanzadas de PDF). Mientras que el PDF y la ISO 32000-1 proporcionan un marco para firmar digitalmente sus documentos, PAdES especifica perfiles precisos para su uso con firma electrónica avanzada en el sentido de la Directiva de la Unión Europea 1999/93/EC. Un beneficio importante de PAdES es que los documentos firmados electrónicamente pueden seguir siendo válidos durante largos períodos de tiempo, incluso si se han roto los algoritmos criptográficos subyacentes. PAdES reconoce que los documentos firmados digitalmente se pueden usar o archivar durante muchos años, incluso muchas décadas. En algunas formas de realización, a pesar de los avances tecnológicos y de otro tipo, debe ser posible validar en cualquier momento el archivo de certificación para confirmar que su firma digital relacionada era válida en el momento de la firma, conociéndose dicho concepto como Validación a Largo Plazo (LTV – *Long-Term Validation*).

Los principios criptográficos comentados en las descripciones anteriores permiten garantizar que la validez de la prueba o evidencia del archivo de certificación firmado digitalmente y con sello (o marca) de tiempo puede serlo durante períodos de tiempo muy largos.

En algunas formas de realización del procedimiento, el servidor de correo electrónico de certificación 104 puede proporcionar una certificación (o prueba o evidencia) del mensaje de correo electrónico entregando al emisor 101 (y/o a una dirección de destino relacionada con el emisor 101) una copia de al menos el archivo de certificación. El archivo PDF del mensaje de correo electrónico también se puede entregar al emisor 101 (y/o a una dirección de destino relacionada con el emisor 101) como parte de la certificación del mensaje de correo electrónico. Esta provisión de la certificación al emisor 101 se puede denominar como certificación de los correos electrónicos enviados.

Alternativamente a o además de entregar al emisor 101 (y/o a una dirección de destino relacionada con el emisor 101) una copia de al menos el archivo de certificación, el servidor de correo electrónico de certificación 104 puede enviar a la dirección de destino una copia de al menos el archivo de certificación. El archivo PDF del mensaje de correo electrónico también se puede entregar a la dirección de destino como parte de la certificación del correo electrónico. Esta provisión de la certificación a la dirección de destino se puede denominar como certificación de los correos electrónicos recibidos.

Según formas de realización de la invención, un mismo emisor 101 puede enviar una pluralidad de correos electrónicos a diferentes destinatarios 107, en cuyo caso el servidor de correo electrónico de certificación 104 puede generar y almacenar para cada uno de dichos correos electrónicos, los correspondientes datos sobre el correo electrónico y su certificación (como se describió anteriormente con referencia a diferentes formas de realización). Todos estos datos sobre cada correo electrónico pueden no comprender la firma y la marca de tiempo de la firma, en cuyo caso el servidor de correo electrónico de certificación 104 puede generar periódicamente datos de certificación (archivos de certificación, etc.) sobre todos los correos electrónicos enviados por el mismo emisor 101. Por ejemplo, el servidor de correo electrónico de certificación 104 puede concatenar todos los archivos de certificación de los correos electrónicos enviados por el emisor 101 durante un período de tiempo razonable, por ejemplo 24 horas, y generar un solo archivo de certificación que comprenda el contenido de todos los archivos de certificación individuales. Por lo tanto, el servidor de correo electrónico de certificación 104 puede firmar digitalmente dicho archivo de certificación único e incluir una marca de tiempo de la firma. Esta certificación de múltiples correos electrónicos hace que el proceso de certificación sea más económico, ya que solo se aplica una firma y una marca de tiempo relacionada para la multiplicidad de correos electrónicos.

En las formas de realización del procedimiento descrito anteriormente, las diferentes etapas que participan en la certificación del correo electrónico se pueden realizar en cualquier orden teniendo en cuenta las posibles dependencias entre ellos. Por ejemplo, la obtención de una huella digital del mensaje de correo electrónico se puede ejecutar antes o después de obtener la dirección de destino del mensaje de correo electrónico. Esto es posible porque la obtención de la huella digital no produce ningún dato o evento requerido en la obtención de la dirección de destino y, de forma equivalente, la obtención de la dirección de destino no produce ningún dato o evento requerido en la obtención de la huella digital. Es decir, la obtención de la huella digital y la obtención de la dirección de destino se pueden ejecutar en cualquier orden entre sí, ya que no existe dependencia entre ellas.

Por otro lado, por ejemplo, la obtención de la huella digital debe ejecutarse antes de generar un archivo de certificación que comprenda al menos la huella digital del correo electrónico, ya que esta segunda etapa requiere datos (la huella digital) que genera la primera etapa. Es decir, se puede entender que la etapa de generar el archivo de certificación depende de la etapa de obtener la huella digital, por lo que no pueden ejecutarse en cualquier orden.

Las formas de realización descritas con referencia a la figura 1 tienen la ventaja de proporcionar al emisor 101 una evidencia de que el servidor de correo electrónico de destino 106 ha recibido el mensaje de correo electrónico, sin notificación al destinatario 107 con respecto a dicha provisión de la evidencia al emisor 101 (y/o a una dirección de destino relacionada con el emisor 101). Es decir, el destinatario 107 no participa en el proceso de proporcionar la evidencia al emisor 101, y el destinatario 107 nunca conoce dicha provisión de la evidencia.

Otra ventaja es que el servidor de correo electrónico emisor 102 y el servidor de correo electrónico de destino 106 pueden ser servidores de correo electrónico convencionales, es decir, que no requieren funcionalidades particulares para, por ejemplo, redirigir el mensaje de correo electrónico dependiendo de una indicación del emisor 101. El servidor de correo electrónico de certificación 104 es el único agente (de los tres servidores necesarios 102, 104, 106) que concentra las características particulares necesarias para realizar las formas de realización del procedimiento descritas previamente, de manera transparente con respecto al servidor de correo electrónico emisor 102 y al servidor de correo electrónico de destino 106 existentes.

La figura 2 muestra el contenido de un archivo PDF que comprende datos que evidencian un mensaje de correo electrónico enviado, de acuerdo con formas de realización de la invención. Este archivo PDF se puede haber generado en un contexto muy similar al descrito en la Figura 1. Por lo tanto, se realizarán algunas referencias a la Figura 1 en la siguiente descripción del archivo PDF representado en la Figura 2. Algunos de los datos mostrados en la Figura 2 han sido enmascarados por razones de privacidad y porque dichos datos enmascarados (direcciones de correo electrónico reales, nombres de host reales y direcciones IP reales) son completamente innecesarios para comprender las formas de realización descritas del procedimiento de certificación.

La figura 2 muestra una primera sección 200 que comprende datos de descripción del mensaje de correo electrónico como, por ejemplo, un identificador único del evento de certificación 201, la fecha 202 en la que se ha recibido el correo electrónico en el servidor de correo electrónico de certificación 104, la dirección de correo electrónico 203 del emisor 101, la IP de origen 204, las direcciones de correo electrónico 205 de los destinatarios 107, el asunto del correo electrónico 206, los nombres de los archivos adjuntos al correo electrónico 207.

La Figura 2 muestra además una segunda sección 208 que comprende datos sobre archivos adjuntos y huellas electrónicas relacionadas con el mensaje de correo electrónico como, por ejemplo, el nombre de un archivo PDF que contiene el mensaje de correo electrónico 209, un valor hash obtenido a partir del archivo PDF que contiene el mensaje de correo electrónico 210, el nombre de cada archivo adjunto al mensaje de correo 211, 213 y los valores hash 212, 214 obtenidos a partir de cada archivo adjunto al mensaje de correo electrónico.

La Figura 2 también muestra una tercera sección 215 que comprende datos sobre la confirmación de la entrega al servidor de correo electrónico de destino como, por ejemplo, la dirección de correo electrónico de cada destinatario 216, detalles sobre la aceptación/rechazo del correo electrónico en el destino 217, la fecha de entrega del correo electrónico 218, y detalles de la transmisión 219.

La figura 3 muestra el contenido del archivo PDF que contiene el mensaje de correo electrónico, cuyo nombre está incluido en la figura 2 e indicado por la referencia 209. No se proporcionan explicaciones detalladas acerca de la figura 3 porque se entiende que su contenido será muy bien entendido por cualquier experto en la materia.

Aunque esta invención se ha divulgado en el contexto de ciertas formas de realización y ejemplos preferidos, los expertos en la técnica entenderán que la presente invención se extiende más allá de las formas de realización descritas específicamente a otras formas de realización alternativas y/o usos de la invención y modificaciones obvias y equivalentes de las mismas.

Además, aunque las formas de realización de la invención descritas con referencia a los dibujos comprenden aparatos informáticos y procesos realizados en aparatos informáticos, la invención también se extiende a programas informáticos, particularmente a programas informáticos en un portador, adaptados para poner en práctica la invención. El programa puede estar en forma de código fuente, código objeto, un código intermedio entre código fuente y objeto tal como en una forma parcialmente compilada, o en cualquier otra forma adecuada para uso en la implementación de los procesos de acuerdo con la invención. El portador puede ser cualquier entidad o dispositivo capaz de portar el programa.

Por ejemplo, el portador puede comprender un medio de almacenamiento, tal como una ROM, por ejemplo una CD ROM o una ROM semiconductora, o un medio de grabación magnética, por ejemplo, un disquete o disco duro. Además, el portador puede ser un portador transmisible tal como una señal eléctrica u óptica, que puede ser transportada a través de un cable eléctrico u óptico o por radio u otros medios.

Cuando el programa se encuentra en una señal que puede ser transmitida directamente por un cable u otro dispositivo o medio, el portador puede estar constituido por dicho cable u otro dispositivo o medio.

Alternativamente, el portador puede ser un circuito integrado en el que el programa está incorporado, estando el circuito integrado adaptado para realizar, o para ser usado en la realización de, los procesos relevantes.

REIVINDICACIONES

1. Un procedimiento de certificar que un mensaje de correo electrónico enviado a través de un servidor de correo electrónico emisor (102) desde un emisor (101) a al menos una dirección de destino ha sido recibido por un servidor de correo electrónico de destino (106) que gestiona la dirección de destino, comprendiendo el procedimiento:

• Proporcionar un servidor de correo electrónico de certificación (104), que realiza:

◦ Recibir el mensaje de correo electrónico enviado a través del servidor de correo electrónico emisor (102) desde el emisor (101) a la dirección de destino, en el que el mensaje de correo electrónico comprende un encabezado del mensaje y un cuerpo del mensaje y en el que el mensaje de correo electrónico comprende, en el campo del encabezado del correo electrónico que se refiere a la dirección de destino, una cadena que comprende una primera sub-cadena concatenada con una segunda sub-cadena, representando la primera sub-cadena la dirección de destino del mensaje de correo electrónico y representando la segunda sub-cadena un nombre de dominio comodín cuyos registros de intercambio de correo (MX) apuntan a una dirección de correo electrónico de certificación por la que será enviado el mensaje de correo electrónico al servidor de correo electrónico de certificación, y en el que recibir el mensaje de correo electrónico enviado por el emisor a la dirección de destino comprende:

▪ Recibir el mensaje de correo electrónico enviado por el emisor a la dirección de destino según los registros MX del nombre de dominio comodín;

◦ Validar una dirección de correo electrónico emisora (101) y verificar que dicha dirección de correo electrónico corresponde a un emisor registrado (101);

◦ En caso de un resultado positivo en la verificación de que la dirección de correo electrónico emisora (101) está registrada:

◦ Obtener una huella digital electrónica del mensaje de correo electrónico;

◦ Obtener la dirección de destino (107) del campo del encabezado del mensaje de correo electrónico que se refiere a la dirección de destino del mensaje de correo electrónico, en el que la dirección de destino se obtiene detectando y eliminando del encabezado del mensaje de correo electrónico que se refiere a la dirección de destino del mensaje de correo electrónico la segunda sub-cadena que representa el nombre de dominio comodín;

◦ Enviar el mensaje de correo electrónico a la dirección de destino obtenida gestionada por el servidor de correo electrónico de destino (106);

◦ Recibir del servidor de correo electrónico de destino (106) una confirmación de aceptación o rechazo del mensaje de correo electrónico;

◦ Generar un archivo de certificación que comprende al menos la huella digital electrónica del mensaje de correo electrónico y la confirmación de la aceptación o rechazo del mensaje de correo electrónico procedente del servidor de correo electrónico de destino (106).

2. El procedimiento según la reivindicación 1, que comprende además:

◦ Almacenar en un repositorio datos relacionados con la huella digital electrónica obtenida del mensaje de correo electrónico y la confirmación de la aceptación o rechazo del correo electrónico recibida desde el servidor de correo electrónico de destino (106).

3. El procedimiento según la reivindicación 2, que comprende además:

◦ Almacenar en el repositorio datos relacionados con al menos uno de los siguientes parámetros:

▪ La dirección de Protocolo de Internet (IP) del servidor de correo electrónico emisor (102);

▪ El nombre de host del servidor de correo electrónico emisor (102) desde el que se recibe el mensaje de correo electrónico;

▪ La dirección de correo electrónico emisora obtenida del encabezado del mensaje de correo electrónico;

▪ El asunto del mensaje de correo electrónico obtenido del encabezado del mensaje de correo electrónico;

▪ La dirección de destino obtenida;

▪ Un identificador único de un evento de certificación;

▪ La fecha y hora en las que el servidor de correo electrónico de certificación recibe el mensaje de correo electrónico;

▪ La fecha y hora en las que se recibe la confirmación de aceptación o rechazo del mensaje de correo electrónico desde el servidor de correo electrónico de destino (106) del servidor de correo electrónico de certificación.

4. El procedimiento según una cualquiera de las reivindicaciones 2 o 3, en el que la generación del archivo de certificación comprende:

▪ Obtener datos almacenados en el repositorio relacionados con al menos la huella digital electrónica obtenida del mensaje de correo electrónico y la confirmación de la aceptación o rechazo del correo electrónico recibida desde el servidor de correo electrónico de destino (106);

▪ Generar un archivo de formato de documento portátil (PDF) a partir de los datos obtenidos.

5. El procedimiento según una cualquiera de las reivindicaciones 1 a 4, que comprende además:

◦ Almacenar en el repositorio la comunicación entre el servidor de correo electrónico de certificación (104) y el servidor de correo electrónico de destino (106) incluyendo la confirmación de la aceptación o rechazo del mensaje de correo electrónico procedente del servidor de correo electrónico de destino (106);

y en el que el archivo de certificación generado comprende además la comunicación almacenada.

6. El procedimiento según una cualquiera de las reivindicaciones 1 a 5, en el que la obtención de la huella digital electrónica del mensaje de correo electrónico comprende:

▪ Generar un archivo de formato de documento portátil (PDF) a partir del mensaje de correo electrónico;

▪ Obtener la huella digital electrónica del archivo PDF.

7. El procedimiento según una cualquiera de las reivindicaciones 1 a 6, en el que el mensaje de correo electrónico comprende al menos un archivo adjunto y el procedimiento comprende además:

◦ Obtener una huella digital electrónica del archivo adjunto;

y en el que el archivo de certificación generado comprende además la huella digital electrónica del archivo adjunto.

8. El procedimiento según una cualquiera de las reivindicaciones 1 a 7, que comprende además:

◦ Firmar digitalmente el archivo de certificación generado.

9. Un servidor de correo electrónico de certificación (104) para certificar que un mensaje de correo electrónico enviado a través de un servidor de correo electrónico emisor (102) desde un emisor (101) a al menos una dirección de destino ha sido recibido por un servidor de correo electrónico de destino (106) que gestiona la dirección de destino, comprendiendo el servidor de correo electrónico de certificación (104):

• Una memoria y un procesador, que incorporan instrucciones almacenadas en la memoria y ejecutables por el procesador, comprendiendo las instrucciones una funcionalidad para:

◦ Recibir el mensaje de correo electrónico enviado a través del servidor de correo electrónico emisor (102) desde el emisor (101) a la dirección de destino, en el que el mensaje de correo electrónico comprende un encabezado del mensaje y un cuerpo del mensaje y en el que el mensaje de correo electrónico comprende, en el campo del encabezado del correo electrónico que se refiere a la dirección de destino, una cadena que comprende una primera sub-cadena concatenada con una segunda sub-cadena, representando la primera sub-cadena la dirección de destino del mensaje de correo electrónico y representando la segunda sub-cadena un nombre de dominio comodín cuyos registros de intercambio de correo (MX) apuntan a una dirección de correo electrónico de certificación por la que será enviado el mensaje de correo electrónico al servidor de correo electrónico de certificación, y en el que recibir el mensaje de correo electrónico enviado por el emisor a la dirección de destino comprende:

▪ Recibir el mensaje de correo electrónico enviado por el emisor a la dirección de destino según los registros MX del nombre de dominio comodín;

◦ Validar una dirección de correo electrónico emisora (101) y verificar que dicha dirección de correo electrónico corresponde a un emisor registrado (101);

◦ En caso de un resultado positivo en la verificación de que la dirección de correo electrónico emisora (101) está registrada:

◦ Obtener una huella digital electrónica del mensaje de correo electrónico;

◦ Obtener la dirección de destino (107) del campo del encabezado del mensaje de correo electrónico que se refiere a la dirección de destino del mensaje de correo electrónico, en el que la dirección de destino se obtiene detectando y eliminando del encabezado del mensaje de correo electrónico que se refiere a la dirección de destino del mensaje de correo electrónico la segunda sub-cadena que representa el nombre de dominio comodín;

◦ Enviar el mensaje de correo electrónico a la dirección de destino obtenida gestionada por el servidor de correo electrónico de destino (106);

◦ Recibir del servidor de correo electrónico de destino (106) una confirmación de la aceptación o rechazo del mensaje de correo electrónico;

◦ Generar un archivo de certificación que comprende al menos la huella digital electrónica del mensaje de correo electrónico y la confirmación de la aceptación o rechazo del mensaje de correo electrónico procedente del servidor de correo electrónico de destino (106).

10. El servidor de correo electrónico de certificación (104) según la reivindicación 9, en el que la huella digital electrónica comprende un valor hash criptográfico.

11. Un sistema informático para certificar que un mensaje de correo electrónico enviado a través de un servidor de correo electrónico emisor (102) desde un emisor (101) a al menos una dirección de destino ha sido recibido por un servidor de correo electrónico de destino (106) que gestiona la dirección de destino, comprendiendo el sistema informático:

◦ Medios informáticos para recibir el mensaje de correo electrónico enviado a través del servidor de correo electrónico emisor (102) desde el emisor (101) a la dirección de destino, en el que el mensaje de correo electrónico

comprende un encabezado del mensaje y un cuerpo del mensaje y en el que el mensaje de correo electrónico comprende, en el campo del encabezado del correo electrónico que se refiere a la dirección de destino, una cadena que comprende una primera sub-cadena concatenada con una segunda sub-cadena, representando la primera sub-cadena la dirección de destino del mensaje de correo electrónico y representando la segunda sub-cadena un nombre de dominio comodín cuyos registros de intercambio de correo (MX) apuntan a una dirección de correo electrónico de certificación por la que será enviado el mensaje de correo electrónico al servidor de correo electrónico de certificación, y en el que medios informáticos para recibir el mensaje de correo electrónico enviado por el emisor (101) a la dirección de destino comprenden medios informáticos para recibir el mensaje de correo electrónico enviado por el emisor (101) a la dirección de destino según los registros MX del nombre de dominio comodín;

◦ Medios informáticos para validar la dirección de correo electrónico emisora (101) y verificar que dicha dirección de correo electrónico corresponde a un emisor registrado (101);

◦ En caso de un resultado positivo en la verificación de que la dirección de correo electrónico emisora (101) está registrada:

◦ Medios informáticos para obtener una huella digital electrónica del mensaje de correo electrónico;

◦ Medios informáticos para obtener la dirección de destino (107) del campo del encabezado del mensaje de correo electrónico que se refiere a la dirección de destino del mensaje de correo electrónico, en el que la dirección de destino se obtiene detectando y eliminando del encabezado del mensaje de correo electrónico que se refiere a la dirección de destino del mensaje de correo electrónico la segunda sub-cadena que representa el nombre de dominio comodín;

◦ Medios informáticos para enviar el mensaje de correo electrónico a la dirección de destino obtenida gestionada por el servidor de correo electrónico de destino (106);

◦ Medios informáticos para recibir del servidor de correo electrónico de destino (106) una confirmación de la aceptación o rechazo del mensaje de correo electrónico;

◦ Medios informáticos para generar un archivo de certificación que comprende al menos la huella digital electrónica del mensaje de correo electrónico y la confirmación de la aceptación o rechazo del mensaje de correo electrónico procedente del servidor de correo electrónico de destino (106).

12. Producto de programa informático que comprende instrucciones de programa para hacer que un sistema informático realice un procedimiento de certificar que un correo electrónico enviado a través de un servidor de correo electrónico emisor (102) desde un emisor (101) a al menos una dirección de destino ha sido recibido por un servidor de correo electrónico de destino (106) que gestiona la dirección de destino, incluyendo dichas instrucciones de programa todas las etapas del procedimiento según una cualquiera de las reivindicaciones 1 a 8.

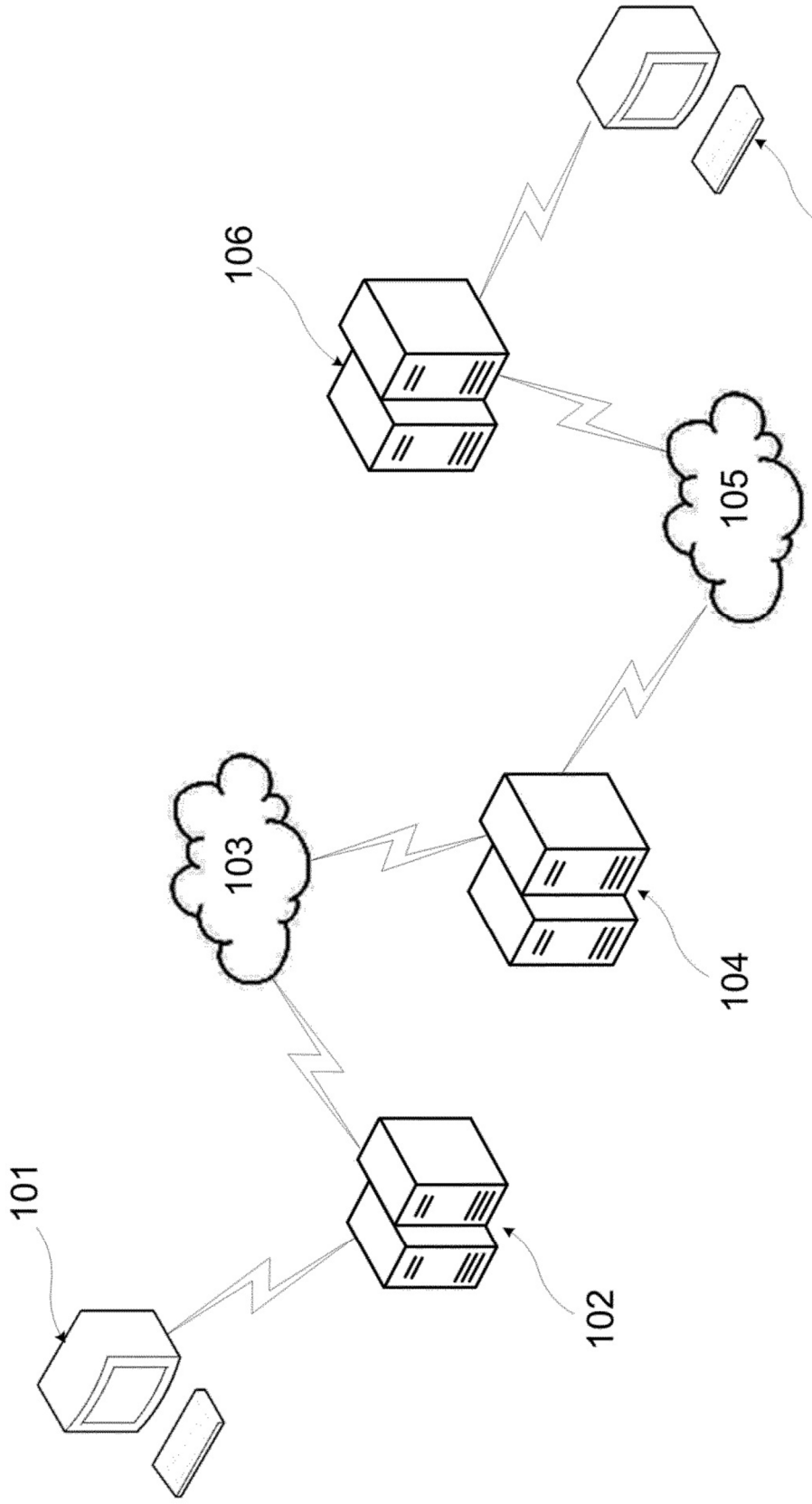

FIG.1

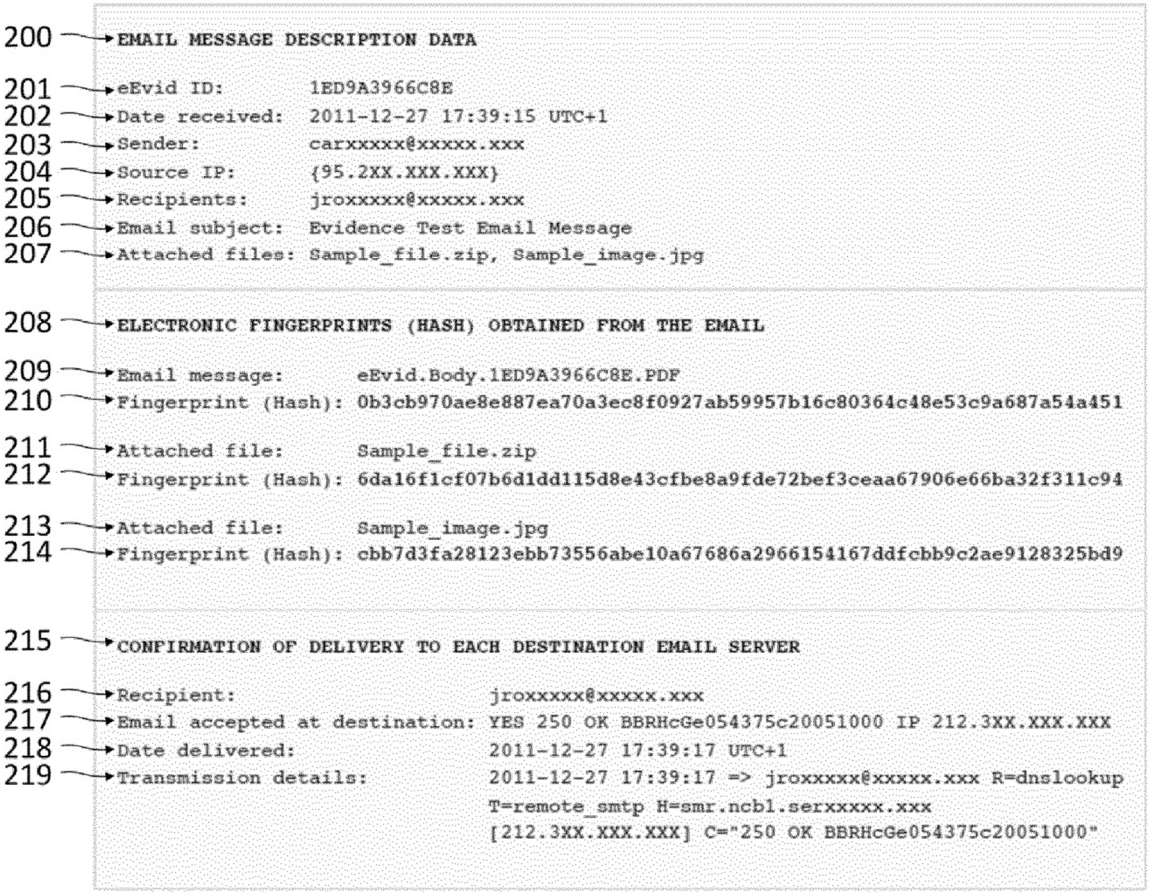
200
EMAIL MESSAGE DESCRIPTION DATA
201
eEvid ID: 1ED9A3966C8E
202
Date received: 2011-12-27 17:39:15 UTC+1
203
Sender: carxxxxx@xxxxx.xxx
204
Source IP: {95.2XX.XXX.XXX}
205
Recipients: jroxxxxx@xxxxx.xxx
206
Email subject: Evidence Test Email Message
207
Attached files: Sample_file.zip, Sample_image.jpg
208
ELECTRONIC FINGERPRINTS (HASH) OBTAINED FROM THE EMAIL
209
Email message: eEvid.Body.1ED9A3966C8E.PDF
210
Fingerprint (Hash): 0b3cb970ae8e887ea70a3ec8f0927ab59957b16c80364c48e53c9a687a54a451
211
Attached file: Sample_file.zip
212
Fingerprint (Hash): 6da16f1cf07b6d1dd115d8e43cfbe8a9fde72bef3ceaa67906e66ba32f311c94
213
Attached file: Sample_image.jpg
214
Fingerprint (Hash): cbb7d3fa28123ebb73556abe10a67686a2966154167ddfcbb9c2ae9128325bd9
215
CONFIRMATION OF DELIVERY TO EACH DESTINATION EMAIL SERVER
216
Recipient: jroxxxxx@xxxxx.xxx
217
Email accepted at destination: YES 250 OK BBRHcGe054375c20051000 IP 212.3XX.XXX.XXX
218
Date delivered: 2011-12-27 17:39:17 UTC+1
219
Transmission details: 2011-12-27 17:39:17 => jroxxxxx@xxxxx.xxx R=dnslookup T=remote_smtp H=smr.ncbl.serxxxxx.xxx [212.3XX.XXX.XXX] C="250 OK BBRHcGe054375c20051000"

FIG.2

```
Hi,

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt
ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamc
o laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit i
n voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupi
datat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Regards,

CT

Return-path:<carxxxxx@xxxxx.xxx>
Envelope-to:hash@evxxxxx.xxx
Delivery-date:Tue, 27 Dec 2011 17:39:15 +0100
Received:from mta5.adm.serxxxxx.xxx ([210.1XX.XXX.XXX] helo=ob3.smr.serxxxxx.xxx)
        by proc1.serxxxxx.xxx with esmtp (Exim 4.76)
        (envelope-from <carxxxxx@xxxxx.xxx>)
        id 1Rfa3X-0002m5-Ml
        for hash@evxxxxx.xxx; Tue, 27 Dec 2011 17:39:15 +0100
Received:from Server_09.serxxxxx.xxx (localhost [227.1XX.XXX.XXX])
        by ob3.smr.serxxxxx.xxx (MTA) with SMTP id 69DFA64047B
        for <hash@evxxxxx.xxx>; Tue, 27 Dec 2011 17:39:15 +0100 (CET)
Received:from (95.2XX.XXX.XXX) by
        serxxxxx.xxx with ESMTP USCSS_Nostromo [JoeL 1.9.2q4c_BBJ] id:<BBRHbfdfebb13a6FBE
36CD>;
        Tue, 27 Dec 2011 17:38:43 +0100 (CET)
X-RealSender:carxxxxx@xxxxx.xxx
X-RealIP:95.2XX.XXX.XXX
X-ToDomain:evxxxxx.xxx
x-m-msg:BBRHbfdfebb13a6FBE36CD
From:CT <carxxxxx@xxxxx.xxx>
Content-Type:multipart/mixed; boundary="Mail=_B3443568-6285-49D7-BAF1-970F50E6D151"
Subject:Evidence Test Email Message
Date:Tue, 27 Dec 2011 17:38:41 +0100
Message-Id:<4B3472A1-2776-442A-B69A-6A98D9A3F744@xxxxx.xxx>
Mime-Version:1.0 (Apple Message framework v1251.1)
X-Mailer:Apple Mail (2.1251.1)
to:jroxxxxx.xxx
```

FIG.3