(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 561 909**

(21) Número de solicitud: 201431264

(51) Int. CI.:

H04L 12/58 (2006.01)
H04L 9/32 (2006.01)

(12) SOLICITUD DE ADICIÓN A LA PATENTE A1

(22) Fecha de presentación:

29.08.2014

(43) Fecha de publicación de la solicitud:

01.03.2016

(61) Número y fecha presentación solicitud principal:

P 201131241 20.07.2011

(71) Solicitantes:

SERVICIOS DE MAIL CERTIFICADO SL (100.0%)
C/ Embajadores 181 B local 9
28045 Madrid ES

(72) Inventor/es:

MARTÍN UGALDE, Carlos

(74) Agente/Representante:

ALESCI NARANJO, Magdalena

(54) Título: **Procedimiento perfeccionado para la verificación de la transmisión y recepción de mensajes en sistemas de comunicación telemáticos**

(57) Resumen:

Mejoras introducidas en la patente española P201131241 "procedimiento para la verificación de la transmisión y recepción de mensajes en sistemas de comunicación telemáticos" donde el remitente del mensaje o usuario del sistema (100) envía un contrato certificado (101) de tal forma que en un segundo servidor (104) se establecen los siguientes procesos: (a) se genera (106) una comunicación firmada y sellada digitalmente (107) tras el envío del correo electrónico por parte del usuario (100); (b) se envía un correo electrónico de notificación al destinatario (110) vía SMTP a los servidores de correo MTA del destinatario (111); y (c) enviar un acuse de recibo 105 firmado y sellado digitalmente tras la petición de acceso (114) o de firma (200); y donde el proceso de firma del destinatario se inicia desde la pasarela de firma (200) en el primer servidor (102) y tras la petición de acceso (114) a la comunicación por parte del destinatario (113).

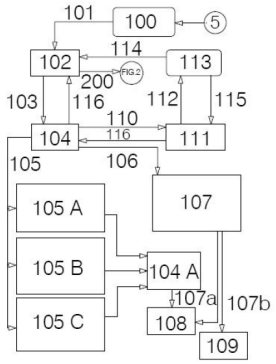

FIG. 1

ES 2 561 909 A1

DESCRIPCIÓN

MEJORAS INTRODUCIDAS EN LA PATENTE ESPAÑOLA P201131241 "PROCEDIMIENTO PARA LA VERIFICACIÓN DE LA TRANSMISIÓN Y RECEPCIÓN DE MENSAJES EN SISTEMAS DE COMUNICACIÓN TELEMÁTICOS"

El objeto de la presente invención es un procedimiento y un sistema que mejora la patente principal española P201131241 introduciendo un nuevo procedimiento para un acuerdo certificado con aceptación expresa por parte del destinatario.

ESTADO DE LA TÉCNICA

Recientemente, el correo electrónico se ha vuelto una herramienta para la comunicación rápida y barata, sobre todo en el ámbito empresarial, en donde se ha convertido en una herramienta insustituible. El correo electrónico, hoy en día, ha logrado desplazar a otros métodos más tradicionales de comunicación, como el correo físico u ordinario y/o el fax, entre otros motivos por su inmediatez, bajo coste y fiabilidad en la entrega.

No obstante, siguen existiendo algunas aplicaciones donde el correo electrónico no ha logrado todavía desplazar al correo físico, 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 y en donde aparecen datos de la persona encargada de la recogida, cosa que no ocurre con los acuses de recibo que pueden incorporar los correos electrónicos (correo-e en adelante en la memoria), ya que dichos recibos contienen escasa información sobre el receptor real y su ubicación. Por tanto, la creación e implantación de sistemas que otorguen una fiabilidad y veracidad a la entrega de correos electrónicos se hace realmente imprescindible.

El funcionamiento del correo electrónico gira alrededor del uso de las casillas de correo electrónico. Cuando se envía un correo electrónico, el mensaje se enruta de servidor a servidor hasta llegar al servidor de correo electrónico del receptor. Más precisamente, el mensaje se envía al servidor del correo electrónico (llamado MTA, del inglés Mail Transport Agent [Agente de Transporte de Correo]) que tiene la tarea de transportarlos hacia el MTA del destinatario. En Internet, los MTA se comunican entre sí usando el protocolo SMTP, y por lo tanto se los llama servidores SMTP (o a veces servidores de correo saliente).

Luego el MTA del destinatario entrega el correo electrónico al servidor del correo entrante

(llamado MDA, del inglés Mail Deliver y Agent [Agente de Entrega de Correo]) , el cual almacena el correo electrónico mientras espera que el usuario lo acepte. Existen dos protocolos principales utilizados para recuperar un correo electrónico de un MDA:

POP3 (Post Office Protocol [Protocolo de Oficina de Correo]), el más antiguo de los dos, que se usa para recuperar el correo electrónico y, en algunos casos, dejar una copia en el servidor.

IMAP (Internet Message Access Protocol [Protocolo de Acceso a Mensajes de Internet]), el cual se usa para coordinar el estado de los correos electrónicos (leído, eliminado, movido) a través de múltiples clientes de correo electrónico. Con IMAP, se guarda una copia de cada mensaje en el servidor, de manera que esta tarea de sincronización se pueda completar.

Usando una analogía del mundo real, los MTA actúan como la oficina de correo (el área de clasificación y de transmisión, que se encarga del transporte del mensaje), mientras que los MDA actúan como casillas de correo, que almacenan mensajes (tanto como les permita su volumen), hasta que los destinatarios controlan su casilla. Esto significa que no es necesario que los destinatarios estén conectados para poder enviarles un correo electrónico. La recuperación del correo se logra a través de un programa de software llamado MUA (Mail User Agent [Agente Usuario de Correo]). Cuando el MUA es un programa instalado en el sistema del usuario, se llama cliente de correo electrónico (tales como Mozilla Thunderbird ®, Microsoft Outlook ®, Lotus Notes ®… etc.).

En el estado de la técnica quedan reflejados varios documentos que intentan solucionar el problema técnico planteado. Así pues, la patente europea EP1476995 (ES2307924T3) describe un método para transmitir un mensaje de un remitente a una dirección de destino que incluye los pasos de recibir el mensaje en un servidor por parte del remitente y transmitir normalmente el mensaje del servidor a la dirección de destino por una primera ruta y que se caracteriza porque se recibe del remitente en el servidor una indicación particular, 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 donde además proporciona la transmisión del mensaje por la segunda ruta a la dirección de destino de acuerdo con la indicación particular del remitente.

Otro documento que se puede encontrar en el estado de la técnica es la patente

WO0211025, que describe un sistema y método para la entrega de verificación y la integridad de un mensaje electrónico, que incluye la recepción de un mensaje electrónico de un remitente del mensaje, el mensaje electrónico que tiene por lo menos una dirección de entrega electrónica asociada a ella, y donde se transmite el mensaje electrónico a dicha dirección designada, recibiendo el estado de entrega electrónico, como una notificación de la información relativa a la entrega del mensaje electrónico a la dirección señalada, calculando un código de autenticación de los mensajes; y montándose posteriormente una copia de por lo menos una parte del mensaje, el estado de la entrega de la notificación, y el código de autenticación de los mensajes.

La patente US6314454, describe un método y dispositivo para certificar correos electrónicos, mediante un receptor interactivo que tiene por lo menos una cuenta de origen y al menos una cuenta de recepción; así como un método para proporcionar direcciones de correo certificado que comprende las etapas de: utilizar un receptor interactivo para generar un mensaje de correo certificado de la cuenta del envío; enviar el mensaje de correo certificado para un servidor de correo configurado para almacenar mensajes certificados de correo electrónico; almacenar el mensaje de correo certificado en un dispositivo de almacenamiento asociado con el servidor de correo; recibir una solicitud de la cuenta receptora para acceder al mensaje de correo certificado; entregar el mensaje de correo certificado del servidor de correo a la cuenta receptora; recibir, desde la cuenta que recibe el servidor de correo, notificación de una medida adoptada en el mensaje de correo electrónico certificado, y notificación selectiva en la cuenta de envío de las medidas adoptadas en el mensaje de correo electrónico certificado por la cuenta receptora.

Por último, la patente US6343313, describe un sistema de conferencias que comprende: al menos un cliente, un servidor de conferencias, por lo menos una conexión de red entre el servidor de conferencias y el cliente; y en donde el cliente mantiene una versión de una parte común de una exhibición; y en donde el servidor de la conferencia es capaz de entregar las actualizaciones de datos en un tipo de salida de datos seleccionados de la base de datos sin comprimir , base de datos comprimidos, diferenciados de datos sin comprimir y diferenciado de datos comprimidos, y en donde el tipo de datos de salida se selecciona basándose en las conexiones de red velocidades y cargas, velocidades de computación de servidores y cargas, y las velocidades de informática de cliente y las cargas, y en donde el servidor de la conferencia es capaz de transmitir la porción compartida de los dichos de la exhibición a dos o más clientes en paralelo.

Ninguno de estos documentos describe un método y un sistema para realizar un acuerdo certificado con aceptación expresa o firma por parte del destinatario.

DESCRIPCIÓN DE LA INVENCIÓN

Es un objeto de la presente invención el envío de un correo certificado con un contenido del que se desea la aceptación expresa por parte del destinatario, pudiéndose adjuntar documentos al envío.

Esencialmente el proceso consta de las siguientes etapas:

a) A través de la plataforma donde está implementada la invención, el cliente o usuario redacta una comunicación utilizando la pagina web o bien inyecta dicha comunicación vía servicios web.
b) Se envía un correo electrónico al destinatario con un enlace para acceder a la comunicación o bien se interpone la plataforma donde está implementada la invención entre la del emisor y el destinatario actuando a modo de pasarela de firma.
c) Se envía un correo electrónico firmado digitalmente y sellado temporalmente al buzón del remitente, que es almacenado en el sistema y del cual se envía copia a un servidor de una notaría asociada a la plataforma donde está implementada la invención.
d) El destinatario recibe el correo electrónico con el enlace
e) Al acceder al enlace, se establece la comunicación como leída y se almacenan los datos de lectura, como dirección IP, hora y fecha, entre otros, enviándolos por correo electrónico firmado digitalmente y sellado temporalmente al buzón del remitente.
f) El destinatario puede aceptar o rechazar la comunicación a través de los medios de firma disponibles.
g) Si el destinatario acepta la comunicación, se almacenan los datos de la firma (al menos IP, hora y fecha) enviándolos por correo electrónico firmado digitalmente y sellado temporalmente al buzón del remitente.
h) Finalmente se envía copia de los documentos firmados al o a los firmantes.

En la firma de las comunicaciones por parte del destinatario se dan varias opciones. Así

tenemos una primera opción que es mediante código único deformado, esto es, que al acceder el destinatario a la página de firma, ésta dispondrá de la suficiente distorsión como para evitar posibles lectores automáticos. El firmante deberá introducir dicho código y, una vez comprobado que se corresponde con el código generado, se dará por aceptada expresamente la comunicación y todos los elementos incluidos en la misma.

Una segunda opción es mediante un código SMS enviado al dispositivo móvil del destinatario. Así, al acceder el destinatario a la página de firma de la comunicación, se le enviará un SMS con un código único asociado a dicha comunicación. El destinatario deberá introducir dicho código para aceptar expresamente la comunicación y todos los elementos incluidos en la misma.

Una tercera opción es mediante firma biométrica que se realizará a través de un servicio que permite recoger datos biométricos de la firma manuscrita de los usuarios e identificar posteriormente a dicha persona por medio de su firma. La firma deberá realizarse en un dispositivo táctil o por medo de una tableta digitilizadora o similar. Existen dos posibilidades para la firma biométrica de las comunicaciones:

- Recogida de datos. En este caso el destinatario firmará la comunicación y el servicio recoge sus datos biométricos de firma y los almacena. Utiliza el grafo de la firma, así como los datos asociados, para firmar la comunicación.
- Identificación a través de la firma. Este método requiere de la inscripción previa del firmante en el servicio de identificación biométrica ya que de este modo será posible la identificación a través de su firma. Para utilizar este servicio, el destinatario deberá disponer de un dispositivo móvil que incluya una aplicación de firma correspondiente a su sistema operativo, así como estar registrado. Cuando acceda a la página de firma, se enviará una solicitud a la aplicación de firma del destinatario. Éste realiza la firma en el dispositivo, cuyos datos se enviarán al servidor de firma, que responderá si la firma introducida corresponde o no a la persona que está firmando. Si la firma es correcta se utilizará el grafo de la firma, así como los datos asociados, para firmar la comunicación.

El servicio de identificación de la firma biométrica proporciona un método de recogida de datos biométricos y de reconocimiento de firma a través de dispositivos móviles. El

funcionamiento sería similar al de una pasarela de pago:

1) Se genera una solicitud de firma en un servidor de biometría con un ID de sesión y le cede el control.
2) El servidor de biometría envía una notificación de firma pendiente al terminal móvil del usuario.
3) El usuario realiza la firma en una aplicación móvil de firma.
4) El servidor de biometría procesa la firma recibida y, dependiendo del tipo de servicio de firma solicitado, retorna los siguientes datos, siempre junto al ID de la sesión:
    a) Captura: retorna los datos biométricos de la firma y el grafo de la firma manuscrita.
    b) Identificación: si la firma es correcta, devuelve los datos biométricos de la firma o el grafo de la firma manuscrita. Si no es correcta, devolverá un error.
5) El servidor de biometría devuelve el control a la web de firma, que analizará los datos de la respuesta.

Para las solicitudes con identificación del firmante, será necesario que éste se haya registrado previamente en el servicio, siguiendo un proceso de sesiones de firma mediante el cual se obtendrá muestra suficiente de la biometría de la firma de la persona de modo que se le pueda identificar en un futuro. En estos casos, el remitente proporciona el NIF del destinatario.

Como se ha indicado previamente, en los casos en que se requiera la identificación del firmante a través del sistema de firma biométrica, se requiere que el destinatario se haya registrado previamente en el servicio, de modo que se tenga información suficiente del mismo como para poder identificarle a través de su firma manuscrita.

El procedimiento para el registro es el siguiente:

1) El usuario descarga la aplicación móvil de firma biométrica.
2) Accede al registro en el sistema y proporciona sus datos personales, al menos nombre, DNI y teléfono.
3) Se vincula la cuenta del usuario al dispositivo utilizado, de modo que las peticiones para el usuario se envíen siempre a dicho dispositivo.
4) El usuario recibirá en su dispositivo móvil tres solicitudes de sesión de firmas para completar el registro, cada una de las cuales supondrá la realización de tres firmas

por parte del cliente y con un intervalo de espera de 24 horas entre sesiones.

5) Para cada una de las sesiones, se codificarán los datos de la firma y se almacenarán en el sistema, para utilizarlas en las identificaciones de firma posteriores.
6) Una vez completada la última sesión de inscripción, el sistema podrá recibir solicitudes de firma para dicho usuario. Cuando se reciba una petición se enviará al usuario una solicitud de firma y el sistema comprobará si la firma introducida corresponde al usuario en cuestión.

Finalmente, una cuarta opción de firma es mediante el empleo de un certificado avanzado, como por ejemplo el DNI electrónico. Este método permite firmar las comunicaciones utilizando certificados reconocidos avanzados. En este proceso, el destinatario accede a la página de firma y utilizando su certificado reconocido avanzado, los medios técnicos necesarios para acceder al dispositivo que lo contiene, así como el código PIN asociado al mismo, procede a la firma digital de los documentos.

A lo largo de la descripción y las reivindicaciones la palabra "comprende" y sus variantes no pretenden excluir otras características técnicas, aditivos, componentes o pasos. Para los expertos en la materia, otros objetos, ventajas y características de la invención se desprenderán en parte de la descripción y en parte de la práctica de la invención. Los siguientes ejemplos y dibujos se proporcionan a modo de ilustración, y no se pretende que restrinjan la presente invención. Además, la presente invención cubre todas las posibles combinaciones de realizaciones particulares y preferidas aquí indicadas.

BREVE DESCRIPCIÓN DE LAS FIGURAS

A continuación se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

FIG.1 – Muestra el diagrama de bloques del proceso para la realización del acuerdo certificado de acuerdo con la presente invención.

FIG.2 – Muestra un diagrama de bloques del proceso de firma del acuerdo certificado de acuerdo con la presente invención.

EXPOSICIÓN DE UN MODO DETALLADO DE REALIZACIÓN DE LA INVENCIÓN

Tal y como se puede observar en las figuras adjuntas, y especialmente en la figura 1, el remitente del mensaje o usuario del sistema 100 envía un contrato certificado 101 a un primer servidor 102 a través del cual se envía 103 la notificación de la comunicación firmada digitalmente y sellada temporalmente a un segundo servidor 104 de correo electrónico o servidor MTA desde el cual se establecen las siguientes acciones:

a) Se genera una comunicación firmada y sellada digitalmente tras el envío del correo electrónico por parte del usuario 100. La comunicación certificada 107 incluye el mensaje de correo electrónico original, incluyendo datos adjuntos, si los hay, además del correo electrónico firmado y sellado temporalmente por el propio sistema, enviándolo 107A al buzón de correo del remitente 108 y enviándolo 107B a su vez a un buzón notarial 109.

b) Se envía un correo electrónico de notificación al destinatario 110 vía SMTP a los servidores de correo MTA del destinatario 111 y ajenos al sistema objeto de la invención, de tal forma que se envía un correo de notificación firmado 112 al destinatario 113 pueda realizar la petición de acceso 114 a la comunicación y a su vez enviar la respuesta 115 a través de su propio servidor de correo 111 de la información DSN y de la repuesta 116 al servidor de correo 104 del sistema.

c) Enviar un acuse de recibo 105 firmado y sellado digitalmente tras la petición de acceso 114 o de firma 200. Los acuses de recibo son los siguientes:

   i) Acuse de entrega de notificación 105a que comprende, al menos, la información DNS, la respuesta del destinatario y el correo firmado y sellado temporalmente.

   ii) Acuse de lectura de comunicación 105b que comprende, al menos, la fecha y la hora de la comunicación, el resultado de la entrega, la IP de lectura y el correo firmado y sellado temporalmente.

   iii) Acuse de firma de comunicación 105c que comprende, al menos, la fecha y la hora de la comunicación, la IP de lectura y el correo firmado y sellado temporalmente.

   Los acuses de recibo (105a, 105b y 105c) se envían al servidor MTA y MDA del sistema (104a) y de ahí al buzón de correo del remitente 108.

El proceso de firma (figura 2) se inicia desde la pasarela de firma 200 en el primer servidor 102 de la invención y tras la petición de acceso 114 a la comunicación por parte del destinatario 113. Se establecen cuatro tipos distintos de firma: código único 201, certificado avanzado 202, SMS 203 y biometría de la firma 204.

Así, mediante el código único, se introduce un código único aleatorio (borroso) que da acceso al servidor de correo certificado 102 de la invención. En el proceso del certificado avanzado 202, se establece una conexión 202a con un lector de tarjetas inteligentes 202b para la firma del documento 202c con un certificado avanzado.

En el proceso de firma mediante SMS 203 se realiza la petición de envío de SMS con código para firma 203a al servidor MTA y MDA 104a de la invención, que a su vez realiza la misma petición 203a al teléfono móvil del destinatario 203b, donde se introduce el código recibido por SMS 203c para completar el proceso de firma.

En el proceso de firma mediante biometría de la firma 204, se envía la solicitud de firma 204a y un servidor de biometría 204b es el encargado de enviar dicha solicitud de firma 204a a un dispositivo táctil de usuario 204c, donde se captura la biometría de la firma manuscrita 204d que se analiza en el servidor de biometría 204b para ser enviados los datos 204e y completar el proceso de firma.

REIVINDICACIONES

1 – Mejoras introducidas en la patente española P201131241 “procedimiento para la verificación de la transmisión y recepción de mensajes en sistemas de comunicación telemáticos” que se caracteriza por que el remitente del mensaje o usuario del sistema (100) envía un contrato certificado (101) a un primer servidor (102) a través del cual se envía (103) la notificación de la comunicación firmada digitalmente y sellada temporalmente a un segundo servidor (104) de correo electrónico o servidor MTA desde el cual se establecen las siguientes acciones:

a) Se genera (106) una comunicación firmada y sellada digitalmente (107) tras el envío del correo electrónico por parte del usuario (100);
b) Se envía un correo electrónico de notificación al destinatario (110) vía SMTP a los servidores de correo MTA del destinatario (111) y ajenos al sistema, de tal forma que se envía un correo de notificación firmado (112) al destinatario (113) pueda realizar la petición de acceso (114) a la comunicación y a su vez enviar la respuesta (115) a través de su propio servidor de correo (111) de la información DSN y de la repuesta (116) al servidor de correo (104) del sistema;
c) Enviar un acuse de recibo 105 firmado y sellado digitalmente tras la petición de acceso (114) o de firma (200);

y donde el proceso de firma del destinatario se inicia desde la pasarela de firma (200) en el primer servidor (102) y tras la petición de acceso (114) a la comunicación por parte del destinatario (113).

2 – El proceso de acuerdo con la reivindicación 1 donde la comunicación firmada y sellada digitalmente (107) incluye el mensaje de correo electrónico original, incluyendo datos adjuntos, si los hay, además del correo electrónico firmado y sellado temporalmente por el propio sistema, enviándolo (107a) al buzón de correo del remitente (108) y enviándolo (107B) a su vez a un buzón notarial (109).

3 – El proceso de acuerdo con cualquiera de las reivindicaciones 1-2 donde los acuses de recibo (105) son los siguientes: acuse de entrega de notificación (105a) que comprende, al menos, la información DSN, la respuesta del destinatario y el correo firmado y sellado temporalmente; acuse de lectura de comunicación (105b) que comprende, al menos, la fecha y la hora de la comunicación, el resultado de la entrega, la IP de lectura y el correo firmado y sellado temporalmente; y acuse de firma de comunicación (105c) que comprende,

al menos, la fecha y la hora de la comunicación, la IP de lectura y el correo firmado y sellado temporalmente; y donde dichos acuses de recibo (105a, 105b y 105c) se envían al servidor MTA y MDA del sistema (104a) y de ahí al buzón de correo del remitente (108).

4 – El proceso de acuerdo con cualquiera de las reivindicaciones anteriores donde el proceso de firma (200) se inicia mediante un código único, donde se introduce un código único aleatorio que da acceso al servidor de correo certificado (102).

5 – El proceso de acuerdo con cualquiera de las reivindicaciones 1-3 donde el proceso de firma (200) comprende el uso de un certificado avanzado (202) y donde se establece una conexión (202a) con un lector de tarjetas inteligentes (202b) para la firma del documento (202c) con un certificado avanzado.

6 - El proceso de acuerdo con cualquiera de las reivindicaciones 1-3 donde el proceso de firma (200) comprende el uso de un SMS (203) se realiza la petición de envío de SMS con código para firma (203a) al servidor MTA y MDA (104a) de la invención, que a su vez realiza la misma petición (203a) al teléfono móvil del destinatario (203b), donde se introduce el código recibido por SMS (203c).

7 - El proceso de acuerdo con cualquiera de las reivindicaciones 1-3 donde el proceso de firma (200) comprende el uso de biometría de la firma (204) y donde se envía la solicitud de firma (204a) de tal forma que un servidor de biometría (204b) es el encargado de enviar dicha solicitud de firma (204a) a un dispositivo táctil de usuario (204c), donde se captura la biometría de la firma manuscrita (204d) que se analiza en el servidor de biometría (204b) para ser enviados los datos (204e).

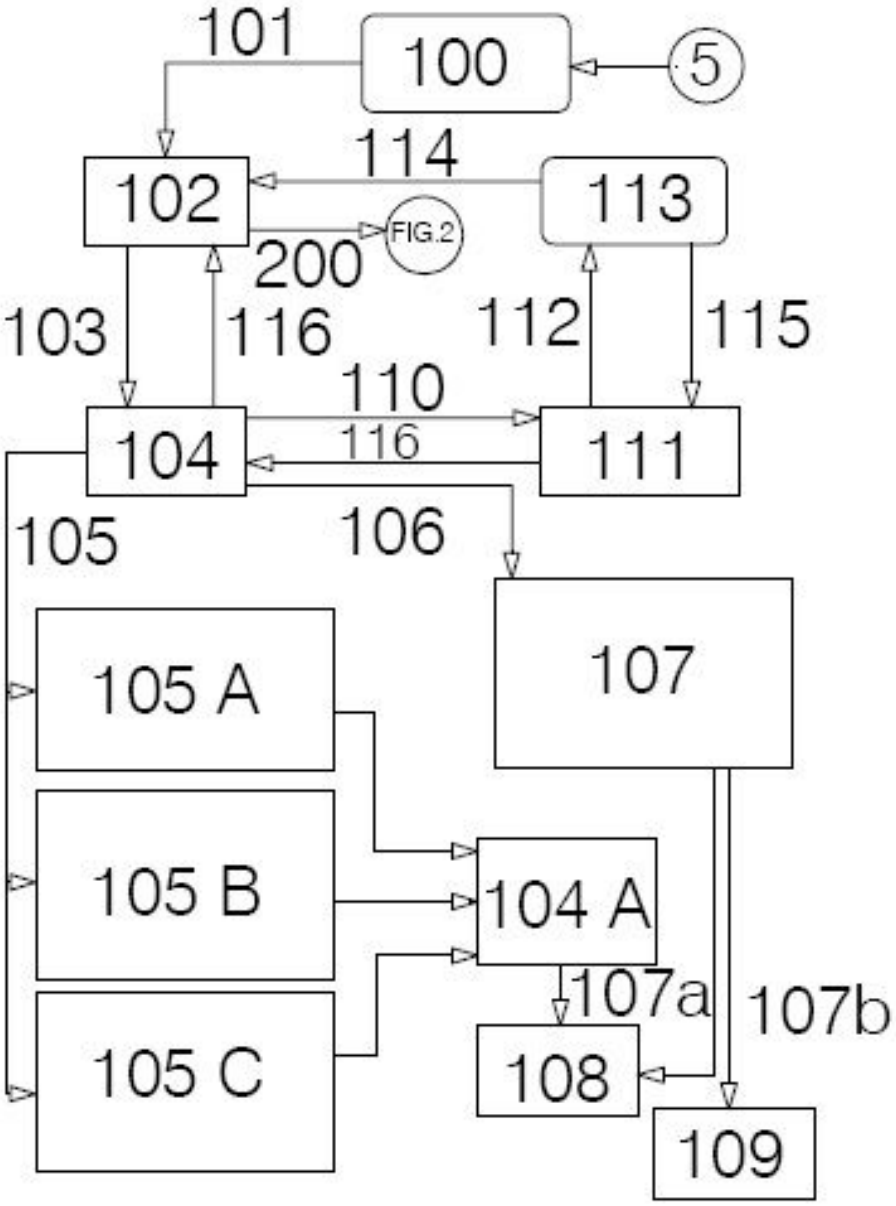
101
100
5
114
102
113
FIG.2
200
103
116
112
115
110
104
116
111
105
106
107
105 A
105 B
104 A
107a
107b
105 C
108
109

FIG. 1

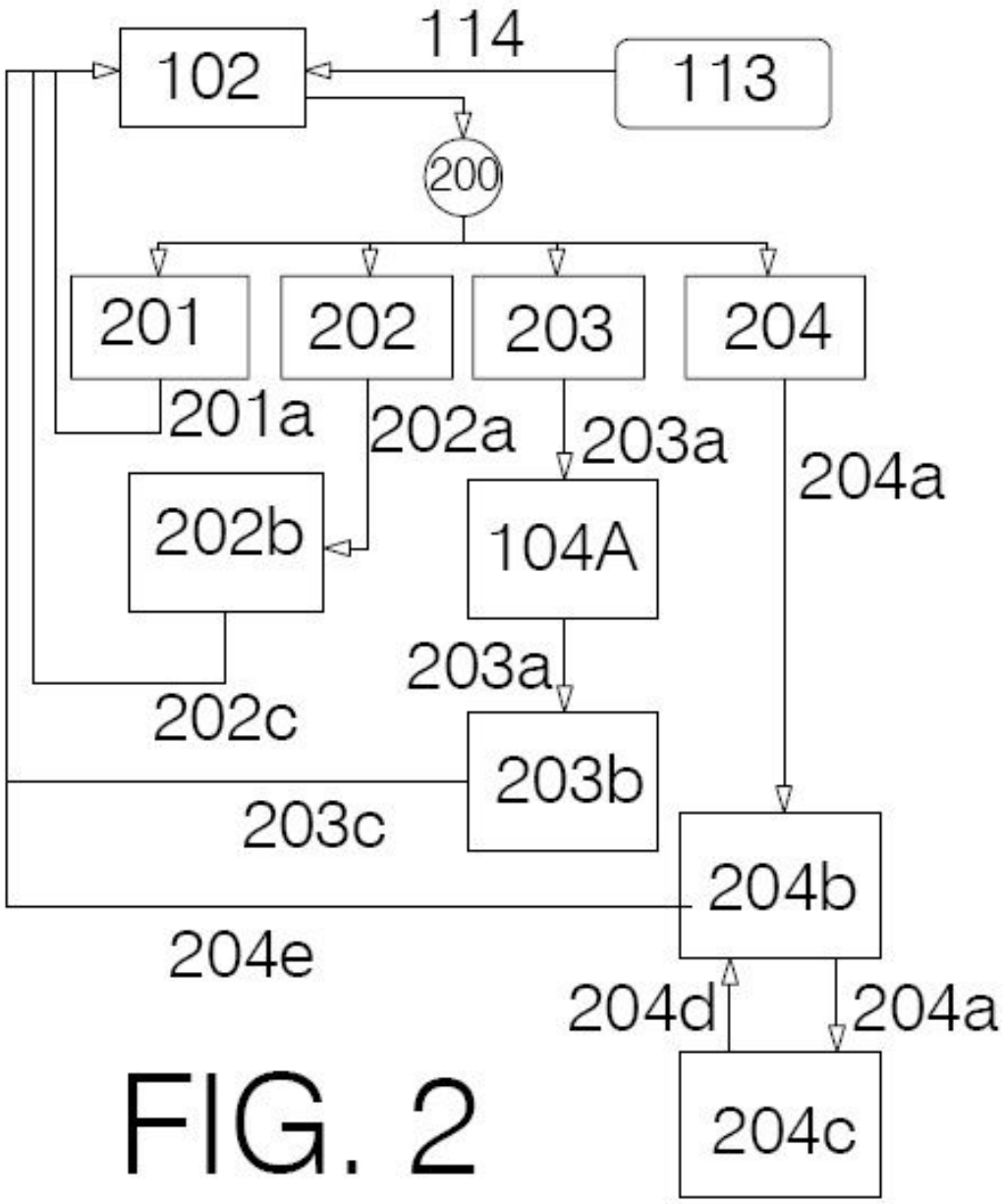
102
114
113
200
201
202
203
204
201a
202a
203a
204a
202b
104A
203a
202c
203b
203c
204b
204e
204d
204a
204c

FIG. 2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201431264

(22) Fecha de presentación de la solicitud: 29.08.2014

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L12/58*** (2006.01)
H04L9/32 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
Y	MAILCERTIFICADO, Correo electrónico, Fax, SMS certificados con validez legal; "Garantizamos tus correos electrónicos; Recuperado de Internet 03.02.2011; Apartados: "Productos - MailCertificado; "Sistema - Bases"; URL:// http://web.archive.org/web/20100323053204/http://www.mailcertificado.com/mailcertificado.html	1-7
Y	ASTORDATA Comercio Electrónico: "Medidas de seguridad para transacciones online"; Artículo descargado: "Cuaderno de notas del observatorio"; escrito por INTECO; Publicado 19.03.2012; URL:// http://www.astordata.com/medidas-de-seguridad-para-transacciones-online/	1-7

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
02.07.2015	B. Pérez García	1/5

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, INSPEC

Fecha de Realización de la Opinión Escrita: 02.07.2015

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1- 7	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1- 7	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	MAILCERTIFICADO, Correo electrónico, Fax, SMS certificados con validez legal; "Garantizamos tus correos electrónicos; Apartados: "Productos - MailCertificado; "Sistema - Bases"	03/02/2011
D02	ASTORDATA Comercio Electrónico: "Medidas de seguridad para transacciones online"; Artículo descargado: "Cuaderno de notas del observatorio"; escrito por INTECO	19/03/2012

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

La solicitud presentada es una adición a la solicitud P201131241.
Se considera D01 el documento del estado de la técnica anterior más próximo al objeto de la invención.
Siguiendo la redacción de la reivindicación 1, el documento D01 describe un procedimiento para la verificación de la transmisión y recepción de mensajes en sistemas de comunicación telemáticos *(certificación de todos los correos que hagas desde la plataforma legal, controlando la situación de los mismos y el acceso)* que se caracteriza porque el remitente del mensaje o usuario del sistema envía un contrato certificado *(correo electrónico certificado)* a un primer servidor a través del cual se envía la notificación de la comunicación firmada digitalmente y sellada temporalmente *(timestamping)* a un segundo servidor de correo electrónico o servidor MTA desde el cual se establecen las siguientes acciones:
a) Se genera una comunicación firmada y sellada digitalmente tras el envío del correo electrónico por parte del usuario *(el sistema establece de forma indubitada la hora y fecha a la que se envían las comunicaciones)*;
b) Se envía un correo electrónico de notificación firmado al destinatario para que pueda realizar la petición de acceso a la comunicación (*con Data Tracking se almacenan todos los hitos de la conversación que se produce con el envío y aceptación de mensajes; se puede avisar al destinatario a su teléfono móvil o fax de la existencia del correo electrónico*) y a su vez enviar la respuesta a través de su propio servidor de correo de la información DSN y de la repuesta al servidor de correo del sistema *(se conoce la fecha y hora de lectura del mensaje, la dirección IP de la máquina desde la que el destinatario accede al mensaje)*;
c) Enviar un acuse de recibo firmado y sellado digitalmente tras la petición de acceso o de firma *(con Data Tracking se almacenan todos los hitos de la conversación que se produce con el envío y aceptación de mensajes; se conoce la fecha y hora de lectura del mensaje, la dirección IP de la máquina desde la que el destinatario accede al mensaje)*;

Existe una diferencia significativa entre D01 y la primera reivindicación. En ésta se añade que el destinatario realiza un proceso de firma tras la petición de acceso a la comunicación.
Esta diferencia produce el efecto técnico de obtener mayor seguridad en la comunicación, ya que se produce la autenticación del destinatario que recibe el mensaje garantizando así que es él a quién iba dirigida esa comunicación.
El problema técnico objetivo es por tanto, cómo estar seguros de que el receptor es el destinatario real del mensaje y que ha recibido éste.

No obstante, estas medidas de seguridad (el proceso de firma) es habitual en comunicaciones electrónicas, transacciones online… como puede apreciarse en el documento D02. No se considera que implique actividad inventiva para un experto en la materia, añadir al proceso de certificación descrito en D01 técnicas de seguridad en transacciones como las divulgadas en D02. Esta reivindicación no cumple el requisito de actividad inventiva, según el Art. 8 de la Ley Española de Patentes.

La segunda reivindicación especifica que la comunicación firmada y sellada digitalmente incluye el mensaje de correo electrónico original, incluyendo datos adjuntos, si los hay, además del correo electrónico firmado y sellado temporalmente por el propio sistema, enviándolo al buzón de correo del remitente y enviándolo a su vez a un buzón notarial.
D01 destaca como una de sus características principales el proceso de inalterabilidad. Mediante el proceso de timestamping se permite demostrar que unos datos han existido y no han sido alterados desde un instante de tiempo. Los mensajes se envían a un buzón notarial propiedad de la empresa Mailcertificado. Carece de actividad inventiva.

Las reivindicación 3 indica el contenido de los acuses de recibo. En D01 –*en qué se fundamenta el funcionamiento de los servicios ofrecidos a través de www.mailcertificado.com*-, se cita el procedimiento de sellado temporal (aplicado al primer acuse de recibo) y la identificación de IP, navegador y S.O. que se añade al segundo acuse de recibo. Este documento anula la actividad inventiva de esta reivindicación.

Las reivindicaciones 4-7 describen diversas técnicas de seguridad en comunicaciones/transacciones online: inserción de un código único aleatorio, utilización de un lector de tarjetas inteligentes, introducción manual de un código previamente enviado en un SMS al usuario o utilización de un servidor biométrico.

Todas estas opciones aparecen descritas en D02 y por tanto, añadirlas al proceso descrito en D01 para proporcionar mayor seguridad al sistema no suponen un esfuerzo inventivo para un experto en la materia.

En resumen, la solicitud presentada no cumple el requisito de actividad inventiva, según el Art. 8 de la Ley Española de Patentes.