



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 271 072**

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

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **01969860 .4**
86 Fecha de presentación : **10.09.2001**
87 Número de publicación de la solicitud: **1317840**
87 Fecha de publicación de la solicitud: **11.06.2003**

54 Título: **Procedimiento para generar evidencias del envío y del recibo por una red de transmisión de datos de un documento electrónico y de su contenido.**

30 Prioridad: **13.09.2000 FR 00 11658**

73 Titular/es: **CERTIMAIL**
139/147 avenue Paul-Vaillant Couturier
93120 La Courneuve, FR
FRANCE TELECOM S.A.

45 Fecha de publicación de la mención BOPI:
16.04.2007

72 Inventor/es: **Vasseur, François-Joseph**

45 Fecha de la publicación del folleto de la patente:
16.04.2007

74 Agente: **Lehmann Novo, María Isabel**

ES 2 271 072 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento para generar evidencias del envío y del recibo por una red de transmisión de datos de un documento electrónico y de su contenido.

La presente invención concierne a un procedimiento para generar evidencias del envío y del recibo por una red de transmisión de datos (por cable de cobre, fibra óptica, hertziano, cable de cualquier otro soporte equivalente, tal como, por ejemplo, Internet) de un documento electrónico y de su contenido.

Un procedimiento de este tipo es conocido del documento CERVENINI, G.; CHESI, M; FANTAUZZI, G.: "A multiprovider, universal, e-mail service for the secure exchange of legally-binding multimedia documents" EURO-COMM 2000. INFORMATION SYSTEMS FOR ENHANCED PUBLIC SAFETY AND SECURITY. IEEE/AFCEA, [Online] - 17 mayo 2000 (2000-05-17) páginas 47-50, XP002178670 Finsiel, Italia ISBN: 0-7803-6323-X Extracto de Internet: URL:<http://ieeexplore.ieee.org> [extraído el 2001-09-27].

Según el estado de la técnica anterior, para obtener la evidencia literal del envío y del recibo de un documento (tal como un acto privado, una carta o documento certificado, acto jurídico documentado de un oficial público), es necesario transcribir el documento sobre un soporte de papel y utilizar una red de distribución propia para este soporte y los modos de evidencia son necesariamente tributarios de ese soporte y de sus exigencias (desplazamientos físicos, costos, lentitud). No existe procedimiento de evidencia electrónica, específicamente de naturaleza convencional, ni de procedimientos de documentos certificados bajo forma electrónica y ninguna de las soluciones tradicionales permite satisfacer, a diferencia del presente procedimiento, las condiciones de validez de una convención de evidencia, de una certificación legal o de un acto legalizado, formalizado específicamente por un acuse electrónico de recibo o de puesta a disposición en los documentos electrónicos y/o ficheros informáticos en forma de un doble certificado asegurado, sin desplazamiento físico, de manera casi instantánea y constantemente accesible.

El presente procedimiento permite pasar del soporte papel para generar las evidencias literales admisibles en justicia que tienen el valor de una presunción simple, convencional o irrefutable, que puede además tener valor de certificado legal o acto jurídico documentado según la cualidad del tercer certificador. Ese procedimiento utiliza específicamente la criptología según una organización particular de sus aplicaciones, que son la transmisión de datos y la creación de sitios y portal bajo modo seguro, las firmas electrónicas avanzadas y los certificados calificados.

De manera sintética, el presente procedimiento de evidencia 1/ genera la evidencia literal de la transmisión por una red de datos segura y del depósito ante una autoridad de certificación de un documento electrónico bajo la forma de un certificado calificado y del registro de su contenido y de sus ficheros adjuntos sobre un soporte inalterable, duradero y no modificable, 2/ transmite ese documento en modo certificado que porta su propia firma electrónica avanzada creada según un procedimiento confiable de identificación por la autoridad de certificación, el mismo garantizando el vínculo entre dicha firma y el documento, así como su transmisión en condiciones normales al destinatario indicado, y 3/ obtiene la evidencia literal de la puesta a disposición de este documento ante el destinatario, formalizado por un acuse de puesta a disposición emitido por dicha autoridad, y, en caso de aceptación por el destinatario, la evidencia convencional e irrefutable del recibo por el destinatario del documento y de su contenido formado por un doble certificado calificado emitido en fecha segura por la autoridad de certificación y garantizado por la misma conteniendo las firmas de las dos partes, esta evidencia siendo formalizada con un acuse de recibo electrónico remitido por la red al Remitente.

En el derecho francés, el presente procedimiento permite crear tanto una evidencia literal en el sentido del artículo 1316-1 del Código civil y reconocido en justicia bajo reserva, en caso de conflicto, de la apreciación de la Autoridad judicial, tanto, en caso de aceptación del documento por su destinatario, imponiéndose a la Autoridad judicial la aplicación de una convención de evidencia en aplicación del artículo 1316-2 del mismo código, garantizado por un tercero, y en el marco de una misión de servicio público, dicho procedimiento constituye un documento certificado en el sentido legal del término (ejemplo: art. L. 122-14 del Código del Trabajo: convocatoria al mantenimiento previo "por carta certificada (L. n°86-1320 del 30 de diciembre de 1986)", Código de la Propiedad Intelectual, Código de procedimiento penal (notificación de las ordenanzas de un Juez de Instrucción), Código de las telecomunicaciones, etc.). Cuando el procedimiento objeto de la patente es organizado, puesto en práctica y garantizado por una entidad que tiene la cualidad de un oficial público, los Acuses de recibo o de puesta a disposición dan fe hasta de un procedimiento de inscripción de fallos, civil o penal, con la diferencia de las presunciones simples donde se puede aportar la evidencia contraria. En tal caso, el producto del presente procedimiento de certificación, llamado en ese caso certificación auténtica, tiene el valor de un acto jurídico documentado.

En derecho comunitario, y específicamente con relación a la Directiva CEE del Parlamento y del Consejo sobre un marco comunitario para las firmas electrónicas del 13 de diciembre de 1999 (en lo adelante la Directiva), el presente procedimiento, puesto en práctica por una autoridad de certificación (o prestataria de servicio de certificación en el sentido del artículo 2(11) y que integra un dispositivo seguro de creación y de verificación de firma electrónica avanzada en el sentido del artículo 2 (2, 6 y 8), produce un doble certificado calificado en el sentido del artículo 2(10) de la Directiva y, en aplicación del artículo 5(b), admisible ante las jurisdicciones de los Estados miembros que portan las características del envío y del contenido de un documento electrónico firmado por el remitente así como su recibo atestiguado por el destinatario o su puesta a disposición atestiguada por la autoridad de certificación.

El procedimiento según la invención es indicado en la reivindicación 1 y está caracterizado porque comprende las etapas y definiciones siguientes, siendo recordado que los términos que comienzan por una mayúscula remiten a las definiciones al final de la descripción:

1. Conexión

1.1. El Remitente que desea obtener la evidencia del envío y del recibo de un documento electrónico se conecta al Sitio a partir de un puesto de trabajo, habiendo puesto previamente bajo la forma de un fichero de tratamiento de texto informático, el documento electrónico que desea transmitir en modo certificado, igual que los ficheros eventuales a adjuntar al envío.

1.2. Desde su conexión, el Remitente es advertido que la integridad del sitio en el cual va a entrar está en modo seguro y que las informaciones recibidas en el marco de ese servicio de certificación son necesarias y sometidas a la legislación protectora de la CNIL.

2. Acogida

2.1. Funcionalmente, el Remitente puede tener acceso, por enlace hipertexto, a (i) una reseña de información general sobre el servicio de certificación con las Condiciones De Uso sin función de aceptación y una base de Fallo a las Preguntas o "FAQ", (ii) la guía del servicio, (iii) informes sobre la Autoridad de certificación y sus compañeros, (iv) la función de Certificación "envío de un e-mail certificado", (v) la función de Revocación "Revocación de Firma de identidad", (vi) la función de creación de una Firma de identidad y de modificación de las características de una Firma de identidad, (vii) el costo del servicio de certificación y (viii) el entorno legal y el valor jurídico de la certificación.

El mismo es reenviado a las Definiciones para el contenido de las funciones.

2.2. Para enviar un e-mail certificado, el Remitente, al clicar sobre el enlace "Envío de un e-mail certificado", es dirigido hacia la página "Envío de un e-mail certificado".

3. Envío de un e-mail certificado

3.1. Identificación del Remitente

Según se trate tanto de un Remitente no referenciado (3.1.1), como de un Usuario, que posee una Firma de Identidad (3.1.2), la persona es dirigida hacia la cualidad adecuada, proponiéndole seleccionar el enlace hipertexto correspondiente.

3.1.1. Remitente no referenciado: proceso de Creación de su Firma de identidad (reenvío a las Definiciones).

3.1.2. Usuario que dispone de una Firma de Identidad. Se precisa que es posible colocar un enlace sobre esta página directamente desde la página de acogida. El Usuario introduce las coordenadas de su Firma de identidad, a saber número de referencia de la Firma de identidad y palabra de pase. Las informaciones correspondientes son exhibidas y el Usuario es invitado a informar a la Autoridad de cualquier modificación posterior. En caso de modificación, se procede a una nueva validación de los datos identificadores de la misma forma que durante la Creación de la Firma de identidad (reenvío a las Definiciones).

3.2. Creación del e-mail certificado

Se efectúa por medio de un formulario en dos partes, uno concerniente al Destinatario (3.2.1) y el otro relativo al contenido del e-mail certificado, sus ficheros adjuntos y las características de la certificación (3.2.2).

3.2.1. Identificación del Destinatario: la Autoridad solicita la dirección electrónica del Destinatario y la verifica por una parte en el seno de su Guía y por otra parte, llegado el caso, ante la base de datos del hospedero de esta dirección o de cualquier base de datos útil. En caso de error o de imposibilidad de referenciar el destinatario, un mensaje de error es indicado al Usuario y le propone las soluciones posibles: verificación de la dirección que le ha sido indicada, otra referencia u otra búsqueda sobre cualquier sitio o bases de datos o abandono y retorno a la acogida (2.1). El proceso continua hasta que el Destinatario haya sido localizado. Se precisa como necesidad que este último no sea, en ese estado, contactado por la Autoridad.

3.2.2. Contenido del e-mail certificado: Se propone al Remitente tanto escribir directamente en el cartón para este efecto el documento que desea certificar, como transmitirlo en fichero de tratamiento de texto o procediendo a la función copiar y luego pegar y en cuyo caso dicho texto es exhibido sobre el mismo cartón y susceptible de nuevas modificaciones. Cuando las eventuales modificaciones son logradas, el Remitente puede insertar en otro cartón los ficheros que pretende adjuntar a su envío, estos se exhiben por su nombre completo. A continuación, se solicita al Remitente si desea un retorno por correo postal del Acuse de recibo y el Aviso de Pasaje.

3.3. Validación, facturación y pago del servicio

3.3.1. Validación: Esas operaciones logradas, el Remitente las valida integralmente así como las Condiciones de uso colocando su Firma de Identidad y sus datos son registrados por la Autoridad de certificación sobre una base de
5 datos duplicada de un registro sobre una base espejo (cluster).

3.3.2. Facturación: la Autoridad de certificación calcula el monto que le es adeudado al usuario por la prestación de la certificación en función de las características del e-mail certificado sobre la base de los costos exhibidos en la página de acogida, y exhibe el resultado. El Remitente puede también en ese estado rechazar la factura y anular el
10 conjunto del proceso de certificación, sin que esta anulación comprenda la Firma de Identidad, distinta del proceso, pero para la cual se propone proceder a su Revocación si tal es el deseo del Usuario. Aceptando la facturación, el Remitente es dirigido, según su selección, tanto hacia el sitio de pago seguro para un pago inmediato (3.3.3.1), como hacia un compromiso de pago diferido (3.3.3.2).

15 3.3.3. Pago

3.3.3.1. Pago en línea inmediato: sitio seguro atendido por un establecimiento autorizado en el sentido de la ley bancaria, que funciona a partir del número y de la fecha de validez de una tarjeta bancaria.

20 3.3.3.2. Compromiso de pago diferido: el Remitente se compromete a pagar la suma debida en el plazo especificado, bajo la forma de cheque, tanto en efectivo, como por transferencia bancaria, y coloca su Firma de identidad sobre este compromiso.

25 3.4. Registro y referencia del e-mail certificado y Transmisión del Acuse de depósito

3.4.1. Registro definitivo: la Autoridad registra sobre la base de datos la totalidad de las informaciones recibidas en un soporte inalterable, duradero y no modificable y procede al mismo registro sobre una base de datos espejo que presenta las mismas características de seguridad, pero fuera de conexión.

30 3.4.2. Creación de un número de referencia del e-mail certificado, transmitido al Remitente en el Acuse de depósito.

3.4.3. Creación del Acuse de depósito (ver Definiciones) y transmisión al Remitente.

35 3.5. Envío al destinatario

3.5.1. Creación del Aviso de Paso: la Autoridad de certificación crea un e-mail seguro que porta su firma y con valor certificado, que toma la forma de un mensaje electrónico.

40 3.5.2. El Aviso de Paso es enviado al Destinatario por la red Internet, a saber mediante intermediarios que responden a números de seguridad de transmisión satisfactoria o, llegado el caso, por la Autoridad de certificación propiamente.

4. Información y creación de los Acuses de recibo o de Puesta a disposición

4.1. Información: el Destinatario recibe en el buzón de cartas electrónico un mensaje de tipo e-mail indicado
45 como siendo de una importancia alta y seguro, llamado "Aviso de paso relativo a un e-mail certificado" y dirigido exclusivamente al Destinatario, titular de esta dirección electrónica, y señalado por un icono que representa el logo de la Autoridad o de su delegado. Cliqueando sobre ese correo electrónico, el destinatario es informado de que es destinatario de un e-mail certificado que está a su disposición sobre el Sitio de la Autoridad con su enlace hipertexto, que puede obtener informaciones tanto cliqueando sobre "saber más" (4.2), como aceptar el mensaje cliqueando en "Aceptar el e-mail certificado" (4.3), como rechazarlo cliqueando sobre "rechazar el e-mail certificado"
50 (4.4).

4.2. Informaciones complementarias: Se explica al Destinatario por una parte el objeto y estatus del servicio de certificación, por otra parte la alternativa que le es propuesta, a saber:

55 - aceptar el e-mail certificado y disponer para este fin de una firma de Identidad gratuitamente que podrá reutilizar para autenticar sus mensajes, precisando que la aceptación del e-mail certificado entraña la autorización expresa por la Autoridad de certificación de hacer constar, en un Acuse de recibo, la aceptación plena y completa, en fecha segura, del contenido del documento y de sus anexos por el Destinatario, ante el Remitente, de conservar esas informaciones
60 durante 30 años y de comunicarlas por decisión de justicia.

- rechazar el e-mail certificado y en cuyo caso le será indicado que ese escrito certificado puede ser aceptado durante un plazo de abertura de dos semanas, con la expiración del cual le será enviado un Aviso de Puesta a disposición a contar del cual se presume haber tenido conocimiento del documento certificado retroactivamente desde la fecha del
65 Aviso de paso. En cualquier estado de causa, el documento certificado se mantiene a su disposición y puede ser siempre aceptado y abierto después del Plazo de abertura, pero bajo la condición de reconocer expresamente la validez de la fecha de recibo el día del Aviso de paso.

Finalmente, le es propuesto un enlace directo hacia la Acogida del Sitio y hacia la Noticia de informaciones del Sitio.

4.3. *Aceptación del e-mail certificado*

El Destinatario cliquea sobre el icono “aceptar el e-mail certificado” y espera la página del Sitio relativa a la Aceptación de los e-mail certificados, sobre la cual debe indicar si es un Usuario y dispone ya de su Firma de Identidad (4.3.1) o si no dispone de la misma (4.3.2), antes de ser dirigido hacia la página “Creación del Acuse de recibo” (4.3.3).

4.3.1. El Destinatario es un Usuario: le es solicitado indicar el número de su Firma de identidad y su código secreto. La Autoridad verifica esas informaciones en la base de datos. Si la verificación es satisfactoria, el Destinatario es enviado a la página de creación del Acuse de recibo.

4.3.2. Creación de la Firma de identidad del destinatario: el Destinatario es enviado hacia la página de Creación de una Firma de identidad (reenvío a las Definiciones) similar al 3.1.1. A la salida, el destinatario, devenido de manera paralela Usuario y habiendo aceptado las Condiciones de uso, pasa por la página de Creación del Acuse de recibo.

4.3.3. Creación del Acuse de recibo: Formulario sobre el cual se exhiben las características del destinatario y el número de referencia del e-mail certificado. En ese estado es también posible anular el proceso de aceptación y, llegado el caso, la Firma de identidad creada por el servicio de revocación. En vistas de ese formulario, el Destinatario acepta definitiva e irrevocablemente el e-mail certificado colocando su Firma de identidad, de conformidad con la convención de evidencia contenida en las Condiciones de uso aceptadas durante la creación de la Firma de identidad.

4.3.4. Registro definitivo del Acuse de recibo: la Autoridad registra en su base de datos la totalidad de las informaciones recibidas en un soporte inalterable, duradero y no modificable y procede al mismo registro en la base de datos espejo que presenta las mismas características de seguridad, pero fuera de conexión.

4.3.5. Abertura del e-mail certificado por el Destinatario, este último pudiendo cargarlo a distancia en su puesto de trabajo si lo desea, siendo precisado que el documento certificado permanecerá consultable ante la Autoridad de certificación indicando el n° de referencia del certificado y la Firma de identidad del Destinatario.

4.4. *Rechazo del e-mail certificado*

4.4.1. Rechazo: El Destinatario que no desea aceptar el e-mail certificado puede clicar sobre el icono “rechazar el e-mail certificado”. La Autoridad expide automáticamente un mensaje informándolo: (1) de la facultad de aceptar posteriormente durante el plazo de apertura de 15 días a contar del envío de este Aviso, e indicando que el documento permanece a su disposición sobre el Sitio de la Autoridad de certificación, (2) que en cualquier caso, a la expiración de ese plazo de apertura, le será enviado un Acuse de Puesta a Disposición a contar del cual el mismo será considerado haber tenido conocimiento de dicho e-mail certificado que se mantendrá no obstante a su disposición.

4.4.2. Ausencia de apertura: después de la expiración del plazo de apertura, envío del Aviso de Puesta a Disposición del 4.4.3. Por solicitud, opción posible de contacto del destinatario por otros medios o atestación por intermediarios en cargados de la transmisión.

4.4.3. Emisión del Aviso de Puesta a Disposición: Con la expiración del Plazo de apertura, la Autoridad envía un Aviso de Puesta a Disposición reiterando los términos del Aviso de Paso, pero declarando el Destinatario considerado haber tenido conocimiento del e-mail certificado retroactivamente a contar de la fecha del Aviso de paso y que esta presunción será formalizada en un Acuse de Puesta a disposición expedido al Remitente y admisible en justicia como evidencia literal.

4.5. Creación por la Autoridad de certificación del Acuse de Puesta a disposición del documento electrónico: la Autoridad de certificación, en un primer tiempo, registra en su base de datos la totalidad de las informaciones recibidas sobre un soporte inalterable, duradero y no modificable y procede al mismo registro sobre una base de datos espejo que presenta las mismas características de seguridad, pero fuera de conexión y, en un segundo tiempo, emite a partir de esas informaciones que atestigua, un certificado calificado simple que constituye el Acuse de Puesta a Disposición. Este Acuse puede mencionar, llegado el caso, un rechazo expreso del Destinatario de aceptar el mail certificado.

5. *Envío del Acuse de Recibo o de Puesta a disposición*

5.1. Acuse de recibo: La Autoridad de certificación transmite por la red al Remitente el Acuse de recibo (ver Definición), eventualmente duplicado, por una orden específica, de un envío por correo postal o por telecopia.

5.2. Acuse de Puesta a Disposición: La Autoridad de certificación transmite por la red al Remitente el Acuse de Puesta a Disposición (ver Definiciones), eventualmente duplicado de un envío por correo postal o telecopia.

Fin del procedimiento de certificación.

Para las necesidades de la presente patente son aplicables las definiciones siguientes a las cuales reenvían los términos que comienzan por una mayúscula:

5 *Acuse de recibo electrónico*: designa la evidencia admisible en justicia de que el destinatario de un e-mail certificado ha aceptado expresamente el recibo, aceptación formalizada por la colocación de su Firma de identidad. El valor de esta evidencia descansa en una convención de evidencia previamente contraída en un marco organizado y/o controlado por una Autoridad de certificación y, en el presente procedimiento de evidencia, insertado en las Condiciones de usos.

10 Formalmente, este acuse de recibo se presenta bajo la forma de un e-mail o mensaje electrónico constituido por un doble certificado calificado, generado por la Autoridad de certificación y que comprende (1) el documento certificado y sus ficheros adjuntos correspondientes al Aviso de paso (primer certificado calificado que contiene la convención de evidencia firmado por el Remitente), (2) el Acuse de recibo electrónico en tanto que comprende la Firma de identidad del destinatario unido irrevocablemente a dicho documento (segundo certificado calificado, duplicado del segundo pero que comprende además la misma convención de evidencia firmada esta vez por el Destinatario) y (3) el certificado de Autoridad de certificación portando en ese doble certificado (1+2) y, llegado el caso, su Certificado público. Por 15 solicitud, el Acuse de recibo es duplicado de un envío en papel con firma manuscrita de un representante capacitado de la Autoridad.

20 Valor jurídico: En derecho francés, el Acuse de recibo electrónico, tal como es generado por el presente procedimiento, es una evidencia establecida en aplicación de una convención de evidencia que se impone a la Autoridad judicial y a la cual no puede ser aportada la evidencia contraria, específicamente en razón de la renuncia a contestar el procedimiento de certificación que constituye la obligación principal de la convención de evidencia. En derecho comunitario y específicamente en aplicación de la Directiva, el Acuse de recibo electrónico se compone de dos certificados calificados en el sentido del artículo 2(10) de la Directiva, admisible ante las jurisdicciones de los Estados 25 miembros en aplicación del artículo 5(b) de la Directiva.

30 *Acuse de depósito*: designa el Certificado calificado simple creado por la Autoridad de certificación que garantiza todas las características del e-mail certificado (el documento, el destinatario, la convención de evidencia y firma del Remitente), registrada de manera de garantizar la integridad sobre un soporte confiable, duradero e infalsificable, según el mejor estado de la técnica. Este Acuse de depósito es transmitido al Remitente por vía electrónica y mantenido a su disposición o a aquel de la Justicia como valor de evidencia del contenido en fecha segura del depósito de un envío certificado y sus características.

35 *Acuse de Puesta a disposición*: consecutivo del Aviso de Puesta a Disposición, designa la evidencia que el destinatario ha estado en grado de captar y por lo tanto de acceder al documento certificado para tomar conocimiento de su contenido. Este Acuse de Puesta a Disposición, certificado calificado simple, hace correr una presunción simple de conocimiento del documento por el destinatario a contar retroactivamente del Aviso de paso. El Acuse de Puesta a Disposición es transmitido al destinatario de la misma manera que el Acuse de recibo. El Acuse de Puesta a Disposición puede comprender además, llegado el caso: (1) la indicación de rechazo expreso por el Destinatario del certificado que 40 demuestra que estaba en grado de aceptar y (2) la atestación de los intermediarios concernidos por la transmisión de la buena transmisión del Aviso de paso hasta la dirección electrónica del Destinatario.

45 Valor jurídico: En derecho francés, el Acuse de Puesta a disposición es una evidencia literal en el sentido del artículo 1316-1 del Código civil, admisible en justicia y que tiene el valor de una presunción simple contra la cual la evidencia contraria puede ser aportada. En derecho comunitaria y específicamente en aplicación de la Directiva, el Acuse de recibo electrónico, que se compone de un solo certificado calificado en el sentido del artículo 2(10) de la Directiva, es admisible ante las jurisdicciones de los Estados miembros en aplicación del artículo 5(b) de la Directiva.

50 *Aviso de Puesta a Disposición*: designa la reiteración del Aviso de Paso, en el cual se adiciona una advertencia clara sobre las consecuencias del rechazo de abertura, específicamente concerniente a la presunción de conocimiento. Previo al Acuse de Puesta a disposición, termina el plazo de abertura y desencadena la presunción simple de conocimiento desde la fecha de envío del Aviso de Paso.

55 Valor jurídico: En derecho francés, el Acuse de Puesta a disposición es una evidencia literal en el sentido del artículo 1316-1 del Código Civil, atestiguado por un tercero, y admisible en justicia pero teniendo solamente el valor de una presunción simple contra la cual la evidencia contraria puede ser aportada. En derecho comunitario, y específicamente con relación a la Directiva, dicho Aviso es un certificado calificado en el sentido del artículo 2(10) de la Directiva, admisible ante las jurisdicciones de los Estados miembros en aplicación del artículo 5(b) de la Directiva.

60 *Aviso de paso electrónico*: designa el e-mail enviado al Destinatario por la red Internet, a saber por intermediarios que responden a normas de seguridad de transmisión satisfactorias o, llegado el caso, por la Autoridad de certificación propiamente. El Aviso de paso es firmado electrónicamente por la Autoridad de certificación al Destinatario. Este e-mail es indicado como siendo de una importancia alta y se distingue específicamente por un icono que representa un signo distintivo de la Autoridad.

65 Cliqueando sobre ese correo electrónico, el destinatario es informado de que él es destinatario de un e-mail certificado que está a su disposición en el Sitio de la Autoridad con su enlace hipertexto, que puede tanto obtener informaciones (remitirse al 4.2. de la Descripción), como aceptar el mensaje (remitirse al 4.3. de la descripción), como

rechazarlo (remitirse al 4.4. de la descripción), esas diferentes selecciones corresponden a enlaces hipertextos hacia las páginas del Sitio concernidas.

Valor jurídico: fija la fecha del inicio del Plazo de apertura y, consecutivamente al Aviso de Puesta a Disposición, marca el punto de partida de la presunción de conocimiento.

En derecho francés, el Aviso de Paso es una evidencia literal atestiguada por un tercero en el sentido del artículo 1316-1 del Código Civil admisible en justicia pero que tiene solamente el valor de una presunción simple contra la cual la evidencia contraria puede ser aportada. En derecho comunitario, y específicamente con relación a la Directiva, dicho Aviso es un certificado calificado en el sentido del artículo 2(10) de la Directiva, admisible ante las jurisdicciones de los Estados miembros en aplicación del artículo 5(b) de la Directiva.

Autoridad de certificación: designa la entidad que organiza y garantiza el presente procedimiento de evidencia, y más particularmente la veracidad de las informaciones contenidas en los instrumentos producidos, a saber la Firma de Identidad, el Aviso de depósito, el Aviso de paso, el Aviso de Puesta a Disposición y los Acuses tanto de recibo, como de Puesta a disposición mediante la emisión de certificados calificados simples y/o dobles relativos a las actas concernidas.

La Autoridad de certificación organiza la creación y la verificación de las Firmas de identidad por un dispositivo seguro de creación y de verificación que asegura la confiabilidad de la identificación del titular, el registro y el archivado según procedimientos seguros y sobre un soporte duradero e inalterable donde se garantiza la integridad, de los e-mails certificados y de su contenido, la transferencia y la puesta a disposición de los destinatarios de los e-mails certificados y el retorno tanto del Acuse de recibo, como del Acuse de Puesta a disposición.

La Autoridad de certificación, sea de derecho privado o público, presenta para el servicio de certificación garantías de confiabilidad en general y en particular empleando personal calificado y experimentado tanto a nivel de la gestión, de la tecnología y de la criptografía de las firmas electrónica, de los certificados calificados simples y dobles y de los procedimientos de seguridad apropiados, aplicando procedimientos y métodos administrativos de gestión conformes a normas reconocidas, asegurando un servicio de guía, un servicio de archivo a disposición de la justicia o por solicitud de los usuarios concernidos (remitente y destinatario) y un servicio de revocación, verificando la identidad de los Usuarios, vigilando tomar medidas contra la falsificación, velando por la confidencialidad de las informaciones recibidas, disponiendo de recursos financieros y seguros contra daños suficientes, específicamente con relación a la responsabilidad vinculada al servicio de certificación frente a Usuarios, registrando las informaciones pertinentes concernientes a la evidencia producida a fin de conservarlas a disposición de la justicia y de los Usuarios concernidos, teniendo cuidado de informar a los Usuarios por un medio de comunicación duradero de las modalidades y condiciones de utilización del servicio de certificación, y, utilizando sistemas confiables para almacenar los certificados expedidos bajo una forma verificable, de manera que solamente las personas autorizadas puedan introducir y modificar los datos, que la información pueda ser controlada en cuanto a su autenticidad, que los certificados estén disponibles al público sólo en caso de consentimiento del titular y que toda modificación que ponga en peligro esas exigencias de seguridad sea aparente para el operador.

Certificado calificado (simple, doble, público)

Simple: designa la atestación electrónica que vincula los datos correspondientes a la verificación de la firma electrónica avanzada a una persona, confirma la identidad de esta persona y el vínculo entre la firma y el documento al que la misma está anexada.

Doble: propio del presente procedimiento de certificación, designa el certificado calificado de una Autoridad de certificación que porta dos firmas avanzadas (ver Firmas de identidad), más particularmente aquella del Remitente y aquella del Destinatario, anexadas a un mismo conjunto de documento compuesto particularmente: (1) de un documento electrónico y/o de los ficheros informáticos, (2) de una convención de evidencia que vincula las partes en ese modo probatorio (ver Condiciones de Usos) y (3) condiciones de transmisión de este conjunto. Técnicamente, la Autoridad genera dos atestaciones bajo la forma de Certificados calificados simples, según las técnicas existentes mas desarrolladas para este fin, su reunión según el presente procedimiento de evidencia que forma el Doble certificado calificado.

Público: designa los certificados simples o dobles, pero emitidos en el marco de una misión de servicio público.

Condiciones de uso: designa las reglas de funcionamiento del servicio de certificación, conteniendo una convención de evidencia, que todos los Usuarios deben aceptar y respetar para obtener y conservar la cualidad del Usuario, así como para dar pleno efecto a los instrumentos generados en su solicitud por el presente procedimiento de evidencia.

Esas condiciones exponen el presente procedimiento, las garantías aportadas por la Autoridad de certificación y las obligaciones a las cuales se suscriben los Usuarios. Ese contrato contiene la convención de evidencia que concluye sucesivamente, por medio y bajo el control de la Autoridad de certificación, el Remitente y el Destinatario durante la creación de su Firma de Identidad y del uso del servicio certificado, las partes renunciando irrevocablemente a actuar en contestación de la perfecta validez de las evidencias generadas por el procedimiento de certificación. Las mismas renuncian específicamente a no actuar en contestación bajo una u otra forma contra el procedimiento de certificación

propia, sus instrumentos y productos, donde más particularmente las Firmas de identidad, y aquellas partes y aquellas de sus futuros corresponsales, y los Avisos y Acuses expedidos por la Autoridad de certificación. Por otro lado, las partes garantizan la exactitud de los datos e informaciones que éstas han proporcionado a la Autoridad de certificación. Finalmente en caso de aceptación del certificado posteriormente al plazo de abertura, el Destinatario reconoce expresamente, por una cláusula para este efecto insertada en las Condiciones de uso, la validez de la fecha de recibo el día del Aviso de paso retroactivamente.

Cada prestación de certificación constituye una aplicación de esta convención de evidencia que vincula las partes y se impone a la Autoridad judicial, específicamente en derecho francés (artículo 1316-2 del Código civil).

Plazo de abertura: designa el plazo de (a modo de ejemplo) dos semanas durante las cuales el destinatario puede seleccionar entre aceptar o rechazar el e-mail certificado. Ese plazo comienza a correr a contar de la fecha de envío del Aviso de Paso al destinatario y se completa con el envío del Aviso de Puesta a Disposición. A su expiración, se presume que el destinatario haya tenido conocimiento del e-mail certificado desde el Aviso de paso.

Destinatario: designa la persona, física o moral, que recibe un Aviso de Paso firmado electrónicamente de parte de la Autoridad de certificación.

Si selecciona acusar recibo del e-mail certificado, el Destinatario deviene un Usuario del servicio de certificación vinculado por una convención de evidencia con el Remitente.

Si lo rechaza o en caso de ausencia de abertura del e-mail certificado, se presumirá haber tenido conocimiento después de la expiración del plazo de abertura, presunción simple establecida por el Acuse de Puesta a Disposición consecutivo al Aviso de Puesta a Disposición.

Directiva: la directiva CEE del Parlamento y del Consejo en un marco comunitario para las firmas electrónicas del 13 de diciembre de 1999, n° 1999/93/CE, JOCE 19/01/2000, n° L 13, p.12.

E-mail certificado: designa el documento firmado electrónicamente por el Remitente y transmitido al Destinatario por la Autoridad de certificación.

Estado: designa la autoridad soberana de un sistema de derecho, específicamente a cargo de la autenticación pública. Ese Estado puede ser uno de los estados miembros de la Unión Europea que aplica la Directiva o un estado fuera de la CEE vinculado por un tratado de reconocimiento en la materia o su equivalente. Por Estado se entiende tanto la administración pública como colectivos locales o equivalente que lo componen.

Remitente: designa la persona, física o moral, autora de un e-mail certificado, que recurre al servicio de certificación.

Puesta a disposición: designa la presunción que pesa sobre el Destinatario después del envío de Puesta a disposición y retroactivamente a contar del Aviso de Paso, según el cual se considera que el mismo ha tenido conocimiento del e-mail certificado, que da así efecto a los documentos que el mismo contiene. Para hacerlo, la Autoridad de certificación garantiza haber ejecutado todos los medios adecuados para informar al Destinatario de que un e-mail certificado le es destinado y que debe aceptarlo jurídicamente por medio de su firma electrónica avanzada, creada gratuitamente y identificándolo individualmente, para abrir el e-mail certificado. En cualquier caso, el documento certificado permanece a su disposición y puede siempre ser aceptado y abierto después del Plazo de abertura, pero bajo condición de reconocer expresamente la validez de la fecha de recibo el día del Aviso de paso.

Valor jurídico: presunción simple de conocimiento del e-mail certificado que puede ser combatida por la evidencia contraria. Esta presunción es materializada por el Acuse de Puesta a Disposición teniendo valor como evidencia literal en derecho francés y calificado en derecho comunitario.

Recomendación: designa el servicio ofrecido por el presente procedimiento, el mismo pudiendo ser privado o público en función de la naturaleza y de las funciones de la Autoridad de certificación.

Revocación: designa el proceso que pone fin a la validez de una firma electrónica, disociando el Usuario de su Firma de identidad. Las Firmas de identidad revocadas no son más garantizadas por la Autoridad de certificación. Con la emisión, los actos efectuados anteriormente a la revocación gracias a la Firma revocada permanecen admitidos y archivados y obligan al Usuario. En lo sucesivo, la Firma revocada no será atribuida a otro y permanecerá en archivos a la disposición del Usuario que la ha revocado, pero bajo una forma pasiva: el usuario no puede servirse de ella y la Firma revocada no es más admisible para identificar a dicho Usuario.

Servicio de certificación: designa la puesta en práctica del procedimiento de evidencia descrito en la presente patente.

Firma de identidad: designa un dato bajo forma electrónica identificando de forma segura su titular por el uso de un procedimiento seguro y confiable de identificación sobre el cual el titular tiene un control exclusivo, garantizando su vínculo con el acta a la cual la misma se adjunta mediante el uso de dispositivos seguros propios para asegurar la

integridad del enlace y del contenido del acta y para conservar en archivos consultables por los Usuarios concernidos o por la Autoridad judicial durante la duración de la validez del acta concernida. Esta firma es propia para cada individuo que se obliga a hacer un uso exclusivamente personal y a no comerciar, así como a preservar la integridad y la confidencialidad con respecto a cualquier tercero además de la autoridad pública de certificación o por conminación de una decisión de justicia. Esta Firma de identidad es intransmisible, tanto por liberalidad o por sucesión, e intransferible. El servicio de creación de firma electrónica puede ser pagado o gratuito sin que la validez sea alcanzada. Sin embargo, en la presente patente, debe ser gratuita la Firma de identidad conferida al Destinatario con el único fin de que éste pueda acusar recibo del e-mail certificado.

Técnica y Valor jurídico: la Firma de identidad es infalsificable, inalterable, trazable y certificada por un tercero mediante la utilización de cualquier medio técnico adecuado. La presente invención no lleva las firmas electrónicas avanzadas o los certificados como tales, sino que las utiliza según el mejor estado de la técnica ya que la misma responde a los criterios de validez nacionales o comunitarios. Sin embargo, a modo solamente de ilustración, esos medios pueden ser procedimientos matemáticos aplicados destinados para proteger la confidencialidad y asegurar la autenticación de los datos del mensaje concernido reemplazándolos o transformándolos en una versión modificada susceptible de ser retransformada en datos originales usando el algoritmo criptográfico y la clave adecuada, el conjunto apuntando a disimular el contenido de los mensajes, a impedir modificaciones y evitar los usos falsificados. Así, en el estado de la técnica, su materialización puede ser un par de claves criptográficas matemáticas aparentadas, compuestas por una parte privada (clave matemática mantenida secreta por el Usuario utilizada para firmar un mensaje electrónico y, según el algoritmo, descifrador de mensajes o ficheros cifrados con la clave pública correspondiente) y una parte pública (clave matemática que puede ser hecha pública, y utilizada para verificar las firma electrónicas generadas con la ayuda de la clave privada correspondiente; según el algoritmo, las claves públicas pueden también servir para cifrar mensajes o ficheros que serán seguidamente descifrados con la clave privada correspondiente), con específicamente una función de condensación (algoritmo que organiza o traduce un conjunto de bits en otro de forma que (1) un mensaje de el mismo resultado cada vez que el algoritmo sea aplicado al mismo mensaje, (2) es matemáticamente imposible deducir o reconstituir el mensaje a partir del resultado de la aplicación de algoritmos, (3) es matemáticamente imposible encontrar dos mensajes diferentes que produzcan el mismo resultado condensado con el mismo algoritmo. En cualquier caso, y cualquiera que sea la técnica utilizada por el presente procedimiento de evidencia, la Firma de Identidad está vinculada de forma inalterable a los datos recibidos durante la Creación de la Firma de identidad, al número de referencia de la Autoridad de certificación y código secreto del Usuario.

Sin embargo, la evolución de las técnicas, específicamente de criptología, excluye una normalización técnica que devendría obsoleta. Por consiguiente conviene referirse a las exigencias planteadas por los textos antes citados que toman en consideración esta exigencia.

La Directiva exige que la firma electrónica avanzada satisfaga los criterios siguientes: estar vinculada únicamente al signatario y permitir identificarlo, ser creada por medios que el signatario pueda guardar bajo su control exclusivo y estar vinculado a los datos con los cuales la misma se relaciona de tal manera que cualquier modificación posterior de los datos sea detectable. Bajo esas condiciones, las firmas electrónicas avanzadas son admisibles como evidencia en justicia bajo la responsabilidad de los Estados miembros, igual que las Firmas de identidad expedidas según el presente procedimiento de evidencia.

El artículo 1316-4 relativo a la firma electrónica exige el uso de un procedimiento confiable de identificación que garantice su vínculo con el acta actual a al cual la misma se adjunta. Un Decreto fijará las condiciones relativas a la creación de la firma, la identificación de la firma y la integridad del acta verificada que permite beneficiar una presunción simple. En cualquier caso, el poder reglamentario está sujeto a respetar los criterios planteados por la Directiva. En consecuencia, e independientemente del contenido del futuro Decreto cuyas condiciones serán inmediatamente tomadas en cuenta, en derecho francés, una firma electrónica que cumpla las condiciones de la Directiva - y por consiguiente una Firma de identidad expedida en el marco del presente procedimiento de evidencia - es admisible en justicia.

Creación de la Firma de identidad: el Usuario debe transmitir los datos siguientes, distintos según se trate de una persona física o moral:

- persona privada: (i) número de tarjeta de identidad, de un pasaporte, de tarjeta de estancia o de residencia o de refugiado o de cualquier otro número que identifique públicamente al Usuario ante un Estado, (ii) su estado civil, a saber nombre y apellido, lugar y fecha de nacimiento, nombres y fecha y lugar de nacimiento de los padres del Usuario (facultativo), dirección electrónica, dirección y teléfono (facultativo) de domicilio, así como el código secreto deseado y la pregunta secreta en caso de olvido del código (es decir: fecha de nacimiento de un ascendiente).

- persona moral: (i) denominación social, (ii) forma social, capital social y número de matrícula ante un Estado miembro (Nº de RCS ante la escribanía del tribunal de comercio competente o equivalente para las sociedades comerciales), (iii) dirección y teléfono (facultativo) de la sede social, (iv) representante legal, a saber sus funciones, cualidades y estado civil reducido al nombre, apellido y número de tarjeta de identidad o equivalente, así como el código secreto deseado y la pregunta secreta en caso de olvido del código.

El control de esas informaciones es efectuado, llegado el caso, por conexión con el banco de datos exterior adecuado.

ES 2 271 072 T3

En caso de error o de incompatibilidad, el Usuario es invitado, por un mensaje de error que le propone continuar o detenerse, a introducir otra vez los datos erróneos o incompatibles. El proceso continuará hasta el abandono o hasta el completo éxito. En ese caso, las informaciones son nuevamente verificadas ante el banco de datos adecuado.

5 Esos datos recibidos son garantizados por el Usuario como siendo exactos, este último declarándose expresamente el único responsable de su veracidad y descargando la Autoridad en caso de error o de falsedad de todas las consecuencias que pueden derivarse. Para hacer esto, el Usuario debe validar las informaciones expuestas en la página.

10 Después de esta validación, el usuario debe consultar y aceptar las Condiciones de Uso. Específicamente éste se obliga a no contestar ni el procedimiento de certificación, ni sus productos, y más particularmente las Firmas de identidad, o sea la suya y aquella de sus futuros correspondientes, y los Avisos y Acuses rendidos por la Autoridad.

15 A la vista de esos datos, de las verificaciones efectuadas y de la aceptación de las Condiciones de Uso, la Autoridad de certificación crea la Firma de identidad por creación de la doble clave y solicita al Usuario el código secreto deseado con validación y su pregunta secreta.

La Autoridad de certificación comunica al Usuario las características de su Firma de identidad, a saber: número de Firma de Identidad, fecha de creación, duración determinada o indeterminada y valor jurídico.

20 *Sitio*: el Sitio designa aquel de la autoridad de certificación. El Sitio es completamente seguro de forma de respetar una completa confidencialidad de las informaciones que están allí contenidas, transmitidas y conservadas en archivos.

25 *Usuario*: designa los usuarios del servicio de certificación, si se trata del Remitente o del Destinatario, desde que este último acepta, para recepcionar el e-mail certificado, las Condiciones de uso. La cualidad del Usuario supone la personalidad jurídica y la capacidad jurídica específicamente con vistas a la convención de evidencia incluida en las Condiciones de uso.

30

35

40

45

50

55

60

65

REIVINDICACIONES

1. Procedimiento para generar evidencias relativas a la transmisión de un documento electrónico entre un remitente y un destinatario, equipados con ordenadores respectivos teniendo los dos acceso a una misma red de transmisión de datos, que comprende:

- una etapa de transmisión del documento que comprende la transmisión en modo seguro del documento electrónico a una autoridad de certificación igualmente equipada con un ordenador unido a la red de transmisión, esta transmisión siendo efectuada en asociación con una dirección electrónica del destinatario y una firma electrónica que identifica de una manera segura al remitente del documento, el remitente habiéndose previamente adherido a una convención de evidencia por la cual renuncia a contestar la validez de esta firma y de los documentos generados por ese procedimiento, provisto de esta firma, dicho procedimiento estando **caracterizado** porque comprende:
- una etapa de archivado efectuada por la autoridad de certificación, que comprende el registro de manera segura del documento electrónico, en asociación con la firma electrónica del remitente, la atribución al documento de un código de identificación, y la emisión con destino al remitente de un mensaje electrónico de acuse de depósito del documento que contiene el código de identificación atribuido al documento,
- una etapa de transmisión de un mensaje de aviso de paso al destinatario del documento, efectuado por la autoridad de certificación, esta etapa comprendiendo la emisión al destinatario de un mensaje electrónico de aviso de paso que indica el código de identificación del documento, y que este está a su disposición durante un período de puesta a disposición predefinido,
- una etapa de transmisión del documento al destinatario por la autoridad de certificación, efectuada por la autoridad de certificación con la condición de una aceptación por el destinatario del recibo del documento, a continuación del recibo del mensaje de aviso de paso, esta etapa comprendiendo la transmisión del documento al destinatario, y la emisión al remitente de un mensaje de acuse de recibo que contiene la indicación que el destinatario ha recibido el documento, asociado a una firma electrónica que identifica de una manera segura el destinatario y garantizando que el destinatario ha aceptado recibir el documento, el destinatario habiéndose adherido previamente a una convención de evidencia por la cual renuncia a contestar la validez de esta firma y de los documentos generados por ese procedimiento, provisto de esta firma, y
- una etapa de rechazo del documento, efectuada en el caso donde el destinatario rechace recibir el documento, o no acepte el mismo al final del período predeterminado, esta etapa comprendiendo la emisión por la autoridad de certificación al remitente en aviso de puesta a disposición del documento.

2. Procedimiento según la reivindicación 1, **caracterizado** porque comprende una etapa previa de atribución al remitente por la autoridad de certificación de una firma electrónica que comprende un número de pieza de identidad oficial, esta etapa comprendiendo la adhesión del remitente a la convención de evidencia por la cual renuncia a contestar la validez de esta firma y de los documentos generados por ese procedimiento, provistos de esta firma, y la memorización en una base de datos accesible al ordenador de la autoridad de certificación, de informaciones de identificación del remitente y de una palabra de pase propia al remitente.

3. Procedimiento según la reivindicación 1 o 2, **caracterizado** porque previamente a la aceptación del documento transmitido por el destinatario, comprende una etapa de atribución al destinatario por la autoridad de certificación de una firma electrónica que comprende un número de pieza de identidad oficial, esta etapa comprendiendo la adhesión del destinatario a la convención de evidencia por la cual renuncia a contestar la validez de esta firma y de los documentos generados por ese procedimiento, provistos de esta firma, y la memorización en una base de datos accesible al ordenador de la autoridad de certificación, de informaciones de identificación del destinatario y de una palabra de pase propia al destinatario.

4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, **caracterizado** porque el mensaje de acuse de recibo contiene además del documento transmitido y el mensaje de aviso de paso con la firma electrónica del remitente, el conjunto que forma con la firma del destinatario un doble certificado autenticado por la autoridad de certificación.

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, **caracterizado** porque el mensaje de aviso de puesta a disposición contiene una indicación que permite determinar si el destinatario del documento ha rechazado expresamente recibir el documento o no ha solicitado el documento durante el período de puesta a disposición predefinido.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, **caracterizado** porque el documento comprende una pluralidad de ficheros informáticos de cualquier tamaño y contenido, que recibe la misma autenticación.

ES 2 271 072 T3

7. Procedimiento según una cualquiera de las reivindicaciones 1 a 6, **caracterizado** porque el documento, así como los mensajes de acuse de depósito, de aviso de paso, de aviso de puesta a disposición y de acuse de recibo son registrados de manera no modificable sobre un soporte inalterable y duradero, así como en una base de datos espejo protegida, no accesible por la red de transmisión.

8. Procedimiento según una cualquiera de las reivindicaciones 1 a 7, **caracterizado** porque los datos transmitidos por el remitente a la autoridad de certificación comprenden informaciones introducidas en un formulario electrónico en línea y ficheros adjuntos, ese formulario siendo completado por informaciones transmitidas por el destinatario si éste acepta recibir el documento, el conjunto formando, con las firmas electrónicas del remitente y del destinatario, el acuse de recibo.

9. Procedimiento según una cualquiera de las reivindicaciones 1 a 8, **caracterizado** porque las transmisiones entre el remitente, la autoridad de certificación y el destinatario son efectuadas en modo seguro SSL, con cifrado de protección contra cualquier falsificación de datos.

10. Procedimiento según una cualquiera de las reivindicaciones 1 a 9, **caracterizado** porque el mensaje de aviso de paso es anónimo, o contiene el nombre del remitente, y eventualmente un título del documento.

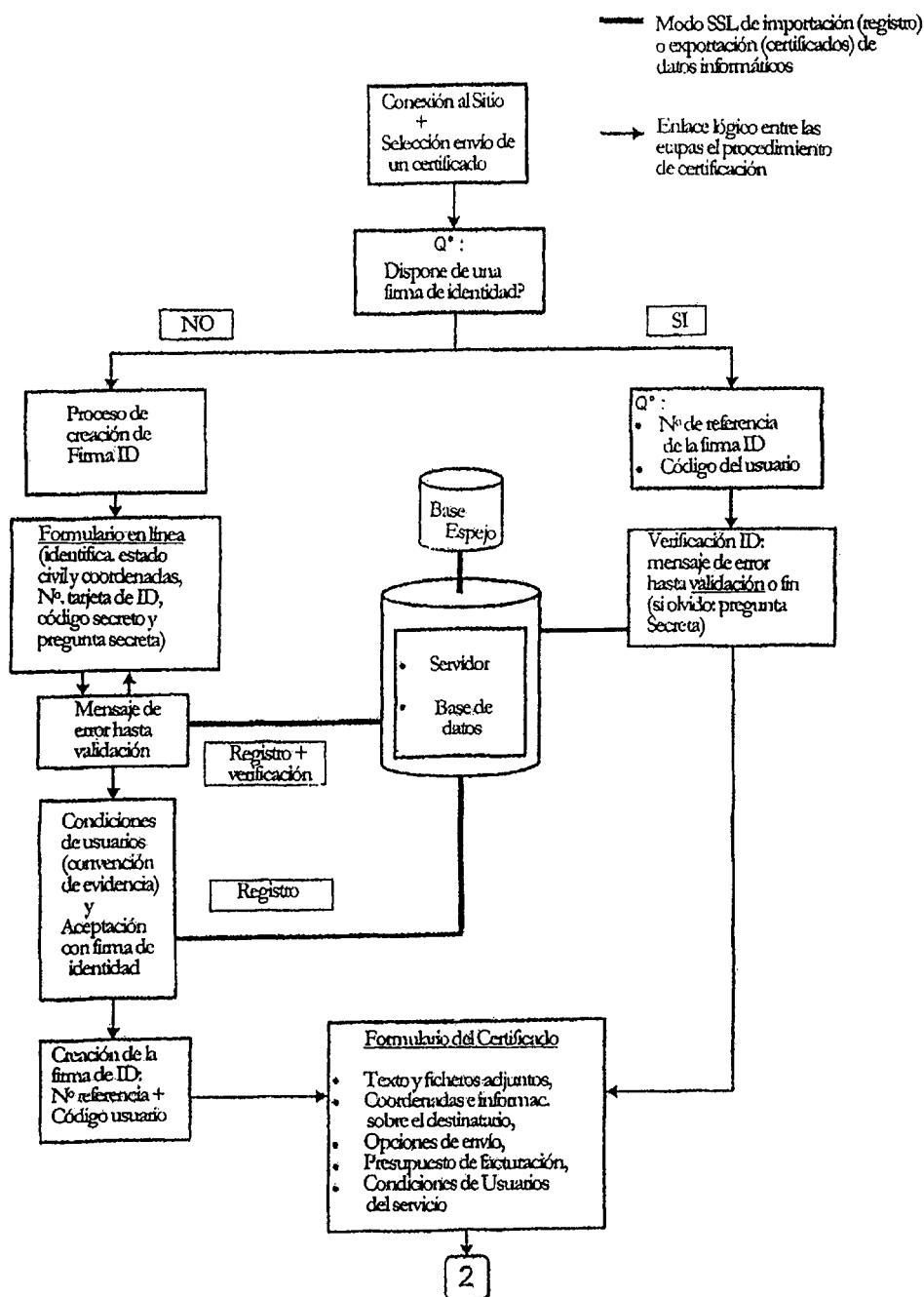


FIG. 1

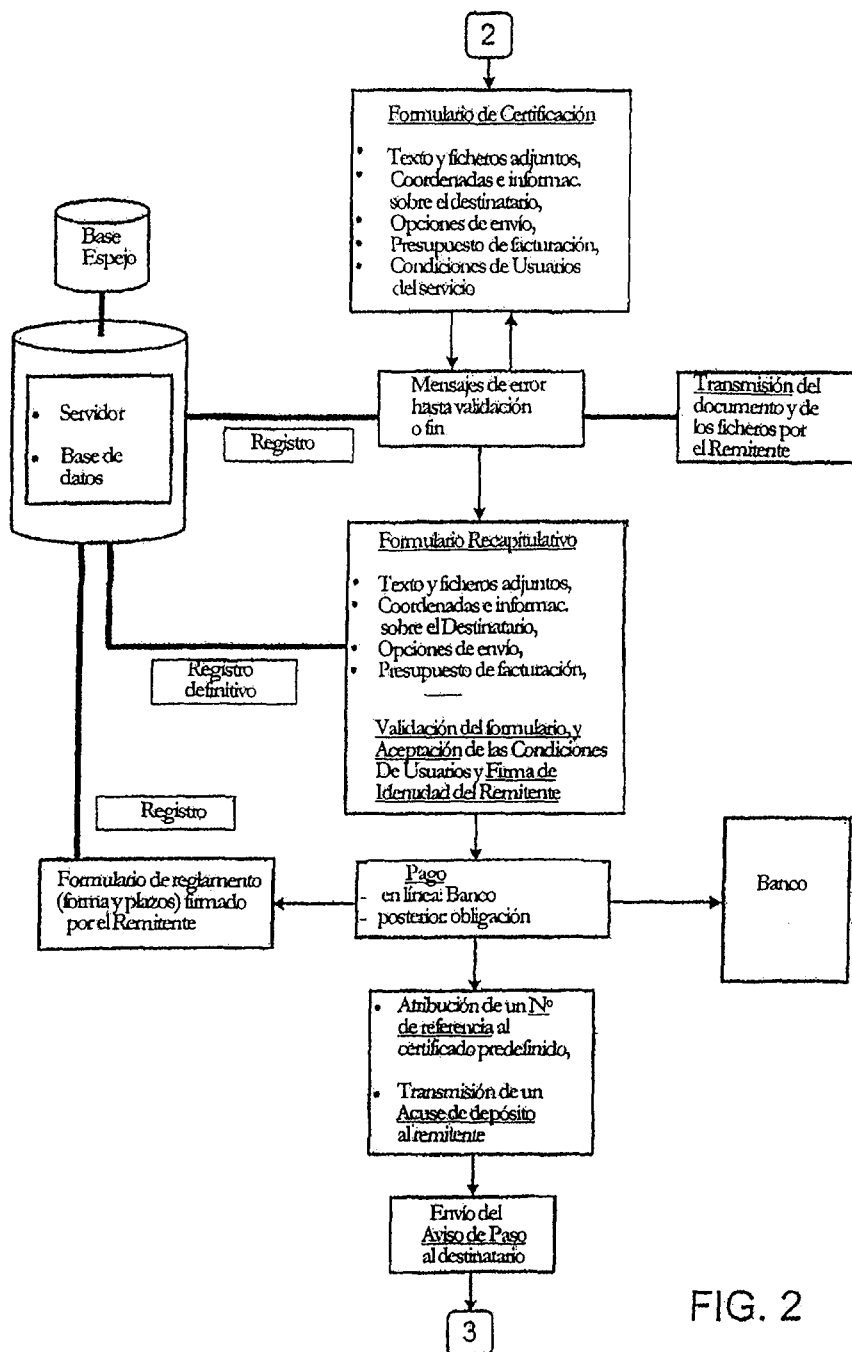


FIG. 2

