

PLATAFORMA Y MÉTODO DE CERTIFICACIÓN DE UNA CONTRATACIÓN ELECTRÓNICA PARA IDENTIFICACIÓN ELECTRÓNICA Y SERVICIOS DE CONFIANZA (EIDAS)

5 OBJETO DE LA INVENCION

El objeto de la invención se enmarca en el campo de las tecnologías de la información y comunicaciones.

- 10 Más concretamente el método aquí descrito está orientado a aplicaciones de certificación de intervinientes, envío, recepción y contenido de documentos electrónicos.

ANTECEDENTES DE LA INVENCION

- 15 El mundo de la certificación y contratación digital ya lleva bastantes años de recorrido, sin embargo hay una confusión generalizada entre los actores del mundo de la certificación digital entre los CA (*Certification Authority*), las firmas digitales, los proveedores de *e-delivery* (entrega electrónica), los procesos de certificación, los procesos que son certificables y los diferentes métodos. Además, los documentos firmados digitalmente
- 20 sólo incluyen información de quién los firma y mantienen inalterado su contenido, pero no contienen la información de su envío, su entrega, su aceptación o no si se utilizan otros medios digitales para aceptar y para firmar digitalmente un contrato.

- El método más habitual para la contratación ha sido la notificación por comparecencia y
- 25 el concentrar todas las acciones utilizando un solo CA, para los certificados, las firmas, y hacerlo todo en una sola ubicación. En sí, es el método que a priori pueda parecer más sencillo, pero el problema surge que se han multiplicado en número de certificados necesarios, lugares en donde firmar y en donde, al hacer notificación por comparecencia, necesitarse hacer presencia digital o acceso periódicamente para evitar perderse
- 30 notificaciones. Sólo en España existen cerca de 80.000 entidades digitales a las que acceder obligatoriamente si se quiere operar a nivel nacional.

Se hace necesario resolver los inconvenientes anteriormente citados, y permitir utilizar cualquier certificado digital que esté configurado en el CA *proxy*, de tal manera que el

proceso pueda iniciarse en cualquier momento tanto por correo electrónico como por SMS; quedando constancia de todos los pasos hechos y de manera que puede demostrarse en todo momento quiénes son los actores del proceso de contratación y cuándo y hasta dónde prosperó el proceso de contratación.

5

Un servicio electrónico de confianza consiste en:

- La creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios.
- 10 • La creación, verificación y validación de certificados para la autenticación de sitios web.
- La preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

- 15 En este sentido se tiene que se establece un marco de identificación electrónica y servicios de confianza, denominado por sus siglas en inglés (eIDAS), mediante la implementación de eIDAS se supervisan los servicios de identificación electrónica y de confianza para las transacciones electrónicas. eIDAS regula las firmas electrónicas, las transacciones electrónicas, los órganos involucrados y sus procesos de inclusión para
- 20 proporcionar una forma segura para que los usuarios realicen negocios en línea como la transferencia electrónica de fondos o las transacciones con los servicios públicos. Tanto el firmante como el destinatario tienen acceso a un mayor nivel de conveniencia y seguridad. En lugar de depender de los métodos tradicionales, como el correo, el servicio de facsímil o aparecer en persona para presentar documentos en papel, ahora pueden
- 25 realizar transacciones transfronterizas, por ejemplo, utilizando la tecnología "1-Click".

- Por lo que la implementación de eIDAS establece unos estándares para los cuales las firmas electrónicas, los certificados digitales calificados, los sellos electrónicos, las marcas de tiempo y otras pruebas para los mecanismos de autenticación permiten
- 30 transacciones electrónicas con la misma legalidad que las transacciones realizadas en papel.

DESCRIPCIÓN DE LA INVENCION

En un primer aspecto de la invención se tiene una plataforma para certificación de contratos electrónicos, plataforma que se implementa mediante un operador de telecomunicaciones haciendo uso de una serie de servidores interconectados. De esta manera se tiene que la plataforma puede presentar una configuración tal que implementa un servidor de contratación que implementa sistemas de contratación electrónica de correo, un servidor de gestión de correo gestión de correo electrónico con recogida de evidencias, un servidor de bases de datos almacena el contenido del correo original, un servidor de sellados de tiempo, un servidor de generación de evidencias recogidas durante el proceso de contratación, un servidor de validación encargado de asegurar la identidad del destinatario mediante el uso de un certificado digital contenido en el navegador del receptor destinatario, un servidor de mensajes certificados, encargado de enviar mensajes, y un servidor de documentos generados destinado al almacenamiento de los certificados de contratación electrónica generados por el servidor de generación de documentos.

Cabe destacar que al estar la plataforma vinculada a un operador de telecomunicaciones (o de comunicaciones a lo largo de este documento), y preferentemente implementada en el mismo, esta permite llevar a cabo tareas de certificación sin necesidad de entidades de red externas al operador de comunicaciones.

En un segundo aspecto de la invención el objeto de la invención está referido a un método en el cual un operador de telecomunicaciones o un proveedor de comunicaciones electrónicas (proveedor de *e-delivery*) pueda enviar contratos por correo electrónico a uno o varios destinatarios, certificando el contenido del contrato y con un enlace a un servidor *proxy* de una CA (*Certification Authority*) que verificará el certificado digital del destinatario y su identidad, reenviando la comunicación a un servidor de contratación en donde podrá verificarse el contrato, aceptarse o no y generar prueba de la transacción como operador de comunicaciones en donde se encuentra el contrato, la entidad contratante, el certificado emitido por la CA relativa a la entidad contratante y todos los datos transaccionales necesarios para demostrar la transacción.

El objeto de la invención provee un método para la certificación de una contratación llevada a cabo de manera electrónica, utilizando la identificación robusta en ambos extremos; en la del cliente mediante un certificado digital de firmas que comprobará el CA (Certification Authority), y en la del proveedor mediante el contrato del servicio al
5 proveedor de *e-delivery*, el operador de comunicaciones o telecomunicaciones, certificando todas las evidencias de las transacciones electrónicas.

Según lo anteriormente comentado, el objeto de la invención es un método de contratación electrónica certificada con la característica de utilizar un proxy de una
10 autoridad de certificación tercera para verificar la identidad del contratante utilizando el certificado digital insertado en el navegador del contratante, certificando todo el proceso mediante un operador de telecomunicaciones o un proveedor de telecomunicaciones, que también puede denominarse proveedor de comunicaciones o proveedor de comunicaciones electrónicas siendo este siempre un proveedor de *e-delivery* o entrega
15 electrónica en castellano. Finalmente el cliente del operador proveedor de comunicaciones electrónicas emisor recibe un certificado conforme a que la contratación ha sido efectuada o no, incluyendo el mail original, el contrato, fecha, hora y trazabilidad del mismo, un número único de transacción y el certificado de la CA (Certification Authority) con los datos de identificación contenidos en el certificado digital contenido en
20 el navegador que identifica unívocamente al contratante.

El método de la invención puede utilizarse para certificaciones de contratos y su contenido y puede ser implementado usando correo electrónico o mensajes tipo SMS.

25 DESCRIPCIÓN DE LOS DIBUJOS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica de la misma, se acompaña como parte integrante de
30 dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

Figura 1.- Muestra un diagrama de flujo donde se representa una realización del método de la invención dirigida a una transacción electrónica relacionada con un contrato

electrónico, estando el proceso iniciado por la entidad emisora para introducir los datos de destino y los datos a verificar para la contratación.

Figura 2.- Muestra un diagrama de flujo donde se representa una realización del método de la invención dirigida a una transacción electrónica relacionada con un contrato electrónico, estando el proceso iniciado mediante un SMS certificado o un SMS.

Figura 3.- Muestra un diagrama de flujo donde se representa una realización del método de la invención dirigida a una transacción electrónica relacionada con un contrato electrónico, estando el proceso iniciado mediante un e-mail certificado o un e-mail.

REALIZACIÓN PREFERENTE DE LA INVENCION

El método para la contratación electrónica objeto de la invención puede implementarse en un plataforma asociada a un proveedor de comunicaciones también objeto de esta invención y accesible a una entidad receptora y una entidad emisora; a la entidad receptora a través de un receptor o un dispositivo receptor (como puede ser un *smartphone* o un ordenador de un receptor), y a la entidad emisora a través de un emisor o un dispositivo emisor (como puede ser un ordenador o dispositivo similar de un emisor) y una serie de servidores interconectados entre sí, dichos servidores pueden ser:

- Un servidor de contratación que denominamos servidor *Conectaclick*, denominado así por ser una solución que implementa sistemas de contratación electrónica como pueden ser sistemas de contratación electrónica utilizando correo electrónico, web y SMS de forma indistinta. Estando servidor de contratación íntimamente vinculado al proveedor de telecomunicaciones o siendo parte del mismo.
- Un servidor de gestión de correo que denominamos *Mailcert*, servidor que permite la gestión de correo electrónico con recogida de evidencias a partir de los mismos, evidencias que pueden incluir entre otros: las cabeceras, el cuerpo y sus adjuntos.
- Un servidor de bases de datos de *Mailcert*, que almacena el contenido del correo original, incluyendo cabeceras, cuerpo y adjuntos, las porciones de

seguimiento o *log* que corresponden al envío y la información de resolución del servidor de correo de destino. Almacena los datos históricos.

- 5 - Un servidor de sellados de tiempo o TSU, *Time Stamp Unit* por su siglas en inglés, sistema de sellado de tiempo implementado *in-situ* ofrecido por una Entidad de Certificación (CA por sus siglas en inglés) para el sellado de tiempo de los documentos, preferiblemente tipo PDF, de evidencias generados por los sistemas de certificación. Este servidor está ubicado preferentemente en la infraestructura del operador de telecomunicaciones pero en determinadas circunstancias, si se requiere, puede ser una entidad de un tercero y por tanto
- 10 estar físicamente ubicada fuera de la infraestructura del operador de telecomunicaciones.
- Un servidor de generación de evidencias que denominaremos servidor TSA, servidor de generación de unos documentos, preferiblemente en formato PDF, que comprenden evidencias resultado de la recopilación de éstas durante el
- 15 proceso de contratación.
- Un servidor de validación que denominaremos *CA validation proxy*, que es un servidor encargado de asegurar la identidad del destinatario mediante el uso de un certificado digital contenido en el navegador del receptor destinatario.
- Un servidor de mensajes certificados, encargado de enviar mensajes desde el
- 20 emisor del contrato al receptor del contrato, preferiblemente SMS, certificados a la red GSM en caso de optar por una realización mediante SMS.
- Un servidor de documentos generados, encargado del almacenamiento masivo de los certificados de contratación electrónica generados.

25 El método para la certificación de una contratación electrónica objeto del segundo aspecto de la invención presenta dos posibles realizaciones diferenciadas entre sí por la utilización de mensajes tipo SMS, tal y como se desprende de la figura 2, o mensajes de correo electrónico, tal y como se desprende de la figura 3; es decir estamos ante un SMS certificado o un correo electrónico certificado (en adelante mail certificado).

30

De esta manera se tiene que el método del segundo aspecto de la invención, permite poder llevar a cabo la generación de un contrato electrónico certificado, donde una entidad emisora, a través de un dispositivo electrónico emisor, como puede su ordenador, accede al servidor de contratación (servidor denominado *conectaclick*)

mediante un acceso a una red de datos como puede ser internet, identificándose como emisor.

5 Una vez autenticado el usuario, introduce los datos del cliente a verificar, el contrato electrónico (en adelante contrato) que quiere efectuar y el número de teléfono o dirección de correo del receptor, que a lo largo de este documento referiremos como receptor o destinatario/destino. La elección de uno u otro tipo de mensaje determinará los pasos a seguir, de esta manera se tiene que:

- 10
- Si se introduce un número de teléfono, se enviará un SMS a través de un servidor de SMS certificados e iniciará el proceso con SMS certificado.
 - Si se introduce un correo electrónico, se enviará un mail certificado a través del servidor *Mailcert* y se iniciará el proceso con mail certificado.

15 El proceso con SMS certificado se inicia al recibir u dispositivo electrónico receptor del destinatario el mensaje el cual tiene capacidad de acceso y comunicación de datos, tal y como puede ser un teléfono inteligente; dicho mensaje contiene una URL (dirección de Internet) que dirige hacia un servidor *proxy* de una Entidad de Certificación (CA) servidor a través del que se efectuará toda la comunicación con el resto de servidores.

20 El proceso con SMS certificado continúa con un acceso por parte del receptor, destinatario, a dicha URL, donde el servidor *proxy* de la Entidad de Certificación (CA) solicita un certificado digital, de entre los posibles contenidos en el navegador del dispositivo receptor, para ser utilizado en la transacción.

25 Si no dispone de certificado digital, no es válido o no se puede acceder al mismo, el servidor *proxy* de la Entidad de Certificación (CA) da por finalizado el proceso y muestra que el proceso no puede continuar generando un fichero de no conformidad que denominamos "CA pdf NOOK" y que preferentemente es en formato PDF que será
30 almacenado en el servidor de PDF generados; de manera opcional se puede añadir a dicho fichero de no conformidad "CA pdf NOOK" un sello de tiempo desde un servidor TSU (*Time Stamp Unit*). Si se dispone del certificado, se procede a extraer una serie de datos que contiene el certificado para su verificación posterior, generando con dichos datos un fichero de conformidad que denominamos "CA pdf OK", asimismo y al igual que

ocurre con el fichero de no conformidad, opcionalmente se puede añadir un sello de tiempo de un servidor TSU (*Time Stamp Unit*) y posteriormente se almacena en el servidor de PDF generados.

- 5 De esta manera, cuando los datos contenidos en el certificado del navegador coinciden con los datos introducidos inicialmente, se procede a mostrar el contrato a firmar. Si el destinatario no acepta el contrato por ejemplo rehusando a su firma, se muestra que el destinatario no ha aceptado y se finaliza el proceso; mientras que si acepta el contrato, se le solicita una dirección de correo electrónico del destinatario para enviarle una copia
10 para el destinatario y se finaliza la sesión con el destinatario.

- Una vez finalizada la sesión con el destinatario el servidor de generación de evidencias - servidor TSA - genera un certificado de la transacción mediante recopilación todos los datos relacionados con la transmisión de datos en internet, el contrato en sí y su
15 contenido, los PDF del CA proxy generados y cualquier dato transaccional de la operativa utilizada. Una vez generado, el certificado resultante se firma con la firma digital del proveedor de comunicaciones y un sello de tiempo a través de un servidor de sellos de tiempo (Servidor TSU).

- 20 El certificado resultante, una vez sellado, se envía al servidor de *Mailcert* encargado de la transmisión del mail, enviando dos copias del certificado del contrato ya firmado y todas las evidencias generadas, una a la entidad emisora, y otro a la entidad receptora, que serán recibidas por los respectivos servidores de correo electrónico para ser
25 recogidas por sus respectivos usuarios.

- En aquellas realizaciones en las cuales el método hace uso de mail certificado o correo electrónico certificado, el método es similar y se inicia al recibir un servidor de correo entrante del destinatario el correo certificado inicialmente enviado, donde dicho correo
30 certificado puede contener un contrato a firmar , pero que contiene una URL (dirección de Internet) que apunta hacia un servidor proxy de una Entidad de Certificación (CA) a través del que se efectuará toda la comunicación con el resto de servidores. El proceso con mail certificado continúa cuando el destinatario, receptor, accede a su correo electrónico a través de su Smartphone u ordenador y accede a la dirección URL incluida

en el mail en donde el servidor CA proxy le preguntará qué certificado digital contenido en el navegador del Smartphone u ordenador que se va a utilizar en la transacción. Si no dispone o no se accede a ellos, el servidor CA proxy muestra que el proceso no puede continuar y generará un fichero CA pdf NOOK en formato PDF y que será almacenado en el servidor de documentos generados al que se podrá añadir un sello de tiempo de un servidor TSU (Time Stamp Unit). Si el navegador dispone del certificado se extraen los datos que contiene para su verificación posterior, generando un fichero CA pdf OK con los datos, se podrá añadir un sello de tiempo de un servidor TSU (Time Stamp Unit) y se almacenará en el servidor de PDF generados. Sigue el proceso cuando el usuario accede al servidor conectaclick a través del CA proxy en donde se verificarán que los datos contenidos en el certificado del navegador coinciden con los datos introducidos inicialmente y se le mostrará el contrato a firmar. Si el destinatario no acepta, se muestra que éste no ha aceptado y se finaliza. Si acepta el contrato se le solicita el email para enviarle su copia y se finaliza su sesión con el destinatario.

Una vez finalizada la sesión con el destinatario el servidor generador de evidencias prepara el certificado de la transacción con todos los datos de internet, el contrato, los pdf del CA proxy generados y cualquier dato transaccional de la operativa utilizada. Una vez completado, el certificado resultante se firma con la firma digital del proveedor de comunicaciones y un sello de tiempo a través de un servidor de sellos de tiempo (Servidor TSU). El certificado generado se envía a un servidor de *Mailcert* encargado de la transmisión del mail, enviando dos copias del certificado del contrato firmado y todas las evidencias generadas, una a la entidad emisora, y otro a la entidad receptora, que serán recibidas por los respectivos servidores de correo electrónico para ser recogidas por sus respectivos usuarios.

Según lo anterior, el método objeto de la invención ofrece la ventaja de que las evidencias y certificados digitales utilizados pueden provenir de diferentes CA o entidades de certificación, en posibles realizaciones alternativas se puede hacer uso de un segundo CA, siendo proveedor del servidor CA proxy, y de un tercer proveedor de *e-delivery* quien es el que se encarga finalmente de empaquetar todas las evidencias de la contratación, generando el certificado de todo el proceso de la contratación.