DIGITELTS
by MADISON

CUMPLIMIENTO EIDAS Y EFICACIA JURÍDICA

Marco Legal del Proceso de Firma Electrónica

DIGITELTS
by MADISON

Índice de Contenido

1 CUMPLIMIENTO EIDAS Y EFICACIA JURÍDICA

Somos **Prestador de Servicios de Confianza Cualificado** para el servicio de expedición de Sellos Electrónicos de Tiempo, incluido en el registro público de la sede electrónica del Ministerio de Asuntos Económicos y Transformación Digital (órgano competente en España en materia de servicios de confianza electrónicos), una entidad especialista en prestación de servicios de consultoría, implantación y explotación de proyectos de transformación digital de la contratación.

Nuestra plataforma de Portal de Firma digital es un sistema orientado a realizar acuerdos contractuales no presenciales mediante notificaciones electrónicas certificadas que requieren de autenticación e identificación de los usuarios, de la puesta a disposición de la documentación contractual y de la recogida del consentimiento a la contratación mediante la utilización de código OTP (ONE TIME PASSWORD), obteniendo de todo el proceso y su confirmación evidencias que son certificadas y cuya custodia es de un mínimo de cinco años.

1.1.1 PROTECCIÓN DE LA IDENTIDAD DE LOS USUARIOS DEL SISTEMA

La garantía de la identidad de los usuarios de la plataforma de firma es una condición básica que el sistema cumple para que sea válido desde el punto de vista jurídico, ya que, a partir de la firma del documento, se despliegan los efectos jurídicos frente a terceros.

Identidad del emisor (entidad cliente)

La identidad del emisor queda garantizada en un grado sustancial suficiente, ya que todas las comunicaciones emitidas pueden ser correctamente firmadas electrónicamente mediante un certificado de sello electrónico cualificado.

Identidad del destinatario (firmante)

Hay que tener en cuenta que la identificación inicial del usuario final (destinatario) depende de la normativa aplicable al proceso de negocio concreto.

Para acceder a la plataforma del portal firma se exige al menos un factor de autenticación, como es el número de DNI, que se introduce a través de la ventana habilitada en el proceso de firma.

Teniendo en cuenta que el factor de autenticación necesario es únicamente el número de DNI del usuario, el sistema utiliza en el momento de la firma un segundo factor de tenencia basado en un código OTP remitido al usuario mediante SMS o email.

De esta forma logramos que la evidencia electrónica asociada al proceso de firmado electrónico del documento aumente sustancialmente los niveles de garantías.

1.1.2 GARANTÍAS DE INTEGRIDAD Y CONFIDENCIALIDAD DEL CONTENIDO

En un proceso de contratación realizado a través de medios electrónicos es importante garantizar la disponibilidad, integridad y confidencialidad de la documentación a entregar al firmante. Para ello, nuestras comunicaciones entre la plataforma de Portal de Firma y los usuarios del sistema (tanto la Entidad Cliente como el destinatario de la documentación/Firmante) se realizan firmando el contenido con un certificado de:

- **INFORMACIÓN DEL FIRMANTE:** EVIDENCIAS ELECTRONICAS DE DIGITEL ON TRUSTED SERVICES.
- **MOMENTO DE LA FIRMA:** DIGITEL ON TRUSTED SERVICES.

Así como cifrando las comunicaciones mediante algoritmos robustos (certificado TLSv1.2 o superior).

Por ello, la integridad del contenido de la contratación y los metadatos asociados quedan protegidos mediante una firma digital soportada por un certificado de:

- **INFORMACIÓN DEL FIRMANTE:** EVIDENCIAS ELECTRONICAS DE DIGITEL ON TRUSTED SERVICES.
- **MOMENTO DE LA FIRMA:** DIGITEL ON TRUSTED SERVICES.

Al que se puede incorporar, además, un sello de tiempo cualificado, de tal forma que queda excluida la posibilidad de que los datos se modifiquen o alteren de forma no autorizada e indetectable.

Las claves criptográficas garantizan y protegen la confidencialidad, integridad y autenticidad de la información. De ahí la importancia de una buena gestión del uso y almacenamiento de éstas.

Garantías de la firma del contrato

Todos estos datos quedan vinculados de forma única a la firma y al documento firmado por el usuario, de forma que no es posible la reutilización de la firma obtenida en otro documento diferente al contrato entregado, ya que, una vez obtenida la firma mediante la introducción de la clave de firma, el sistema emplea un doble sistema de seguridad encaminado a lograr garantizar la integridad de toda la información asociada a la firma en sí y al documento en general.

Por un lado, tanto el hash del contrato, como la firma mediante código OTP asociada a éste, e incluidos como metadatos de la firma, son firmados electrónicamente mediante un certificado de firma electrónica, con la única finalidad de garantizar la plena integridad y no modificación de los datos.

Dicha firma mediante certificado electrónico es directamente aplicada, de forma completamente automática, en el mismo momento que el usuario finaliza la firma mediante su clave de firma, realizándose una petición al servidor donde se encuentra alojado el sistema, y respondiendo éste de forma completamente automática e inmediata.

Garantías de temporalidad

Para poder acreditar el momento en que un determinado hecho ocurre en el tiempo, el eIDAS regula los “sellos cualificados de tiempo electrónicos” que, de cumplir las condiciones estipuladas para su creación, “disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas”.

Por tanto, el empleo de este tipo de sello de tiempo es suficiente para garantizar la prueba sobre el momento en que se produce la firma del documento.

El proceso puede aplicar un sellado de tiempo electrónico cualificado sobre los documentos firmados por los usuarios, lo que garantizará el momento exacto en el que se llevó a cabo la firma del contrato en cuestión.

Recopilación de evidencias

La evidencia o prueba electrónica puede definirse como el soporte susceptible de almacenar información digital con la finalidad de acreditar hechos ante los Tribunales.

Para asegurar la admisibilidad de la prueba electrónica en un proceso judicial, han de cumplirse los siguientes requisitos:

1) **Licitud:** La prueba electrónica ha de obtenerse de forma lícita, sin vulnerar el derecho a la intimidad y el secreto de las comunicaciones que garantiza el art. 18 de la Constitución Española.
2) **Autenticidad:** Debe garantizarse que la prueba es auténtica, es decir, que lo que se analiza es exactamente lo ocupado en la actuación, lo que requiere que se haya realizado adecuadamente la cadena de custodia
3) **Integridad:** Dada la extremada mutabilidad de las pruebas electrónicas, es necesario preservar la integridad de los medios de almacenamiento originales, no alterando su contenido, siendo por tanto esencial emplear sistemas que garanticen que no es posible la modificación del contenido.
4) **Claridad:** El componente tecnológico de la prueba electrónica hace que los expertos deban presentarla ante los Tribunales de forma clara y comprensible, para que personas legas en informática puedan comprenderla.

En nuestro Portal de Firma se registran **los eventos producidos** en el servicio de contratación electrónica y se conservan al menos los siguientes:

1) datos de identificación de emisor y destinatario; incluidos los eventos e información de verificación de la identidad;
2) datos de autenticación de emisor y destinatario; incluidos los eventos e información de verificación de la autenticidad;
3) registros de operación, verificación de identidad del emisor y destinatario, y comunicación;
4) prueba de la verificación de identidad del destinatario antes del envío/traspaso de la documentación;
5) demostrar que la documentación no se ha modificado durante la transmisión;
6) una referencia o una recopilación completa de la documentación presentada;
7) tokens de sello de tiempo correspondientes a la fecha y hora de envío, consignación y entrega y en su caso, modificación de la documentación.

Las evidencias se muestran en el **certificado final** que queda a disposición del firmante serán:

1) Puesta a disposición de la documentación y firma de la misma para garantizar su integridad.
2) Acceso del firmante.
3) Firma del firmante.
4) Entrega de la documentación firmada.

Cumplimiento de la normativa de protección de datos

El almacenamiento de la firma del cliente supone un tratamiento de datos personales, definidos en el RGPD como “toda información sobre una persona física identificada o identificable”. El responsable del tratamiento de estos datos será la Entidad Cliente de nuestra plataforma Portal de Firma. Este

tratamiento de los datos personales debe ser puesto en conocimiento del firmante, informándole de:

1) la identidad y los datos de contacto del responsable;
2) los datos de contacto del delegado de protección de datos, en su caso;
3) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
4) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
5) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
6) sus derechos respecto del tratamiento de los datos personales (Todo ello, con el nivel de detalle establecido en el RGPD y la LOPDGDD).

Por su parte, en lo que se refiere a la contratación para la prestación de servicios relacionados con la firma de las Entidades Clientes del sistema (especialmente en relación con la custodia de las propias firmas y los documentos firmados), debe tenerse en cuenta que, por tener esta la consideración de dato personal, su tratamiento por nuestra parte le confiere la condición de Encargado de Tratamiento y que, por tanto, de acuerdo a lo establecido en el RGPD, la realización de estos tratamientos estará regulada en un contrato (de forma que se permita acreditar su celebración y contenido) que establezca expresamente el tipo de datos tratados y las categorías de interesados, que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará a terceros. Así mismo, deberán hacerse constar las medidas de seguridad aplicables.

1.1.3 EVALUACIÓN DE CUMPLIMIENTO

Considerando lo expuesto en el presente Informe, **se pueden extraer las siguientes conclusiones:**

1) **Nuestra plataforma de firma se centra en la puesta a disposición del servicio** para que los Clientes del servicio puedan enviar a través de ésta, por medios electrónicos, la documentación contractual pertinente a sus clientes, y éstos podrán, con la **garantía de integridad y confidencialidad** requerida, aceptarla y firmarla.

2) Nuestra plataforma de firma recoge todas las **evidencias,** consigna la **fecha y hora de estas y custodia la información de forma adecuada.**

   Concretamente, las **garantías básicas** que debe reunir el nuestro sistema de firma para tener eficacia jurídica son las garantías de disponibilidad integridad, y confidencialidad.

   Para ello, **recogemos y certificamos las evidencias** producidas durante el proceso, y emite un certificado final firmado utilizando un certificado de firma electrónica e incorporándole un sello de tiempo.

   Según se ha indicado, la configuración del Portal de Firma se encuentra establecida de forma que las comunicaciones se realizan a través del **protocolo de comunicación SSL**, lo que garantiza que todas las comunicaciones entre los usuarios del sistema y el portal cumplen íntegramente con los requisitos de seguridad necesarios para garantizar la integridad de la información, así como la identidad del equipo emisor de la comunicación.

3) La **identificación inicial del Firmante** de la documentación depende de la Entidad Cliente de la Plataforma del Portal de Firma, y será más o menos exigente en función de sus **protocolos y políticas de servicio y el nivel de seguridad** que estime conveniente y deba asumir en función de la normativa que le aplique.

4) El **destinatario de la documentación podrá acceder a la plataforma** mediante la **introducción del código de usuario,** que será conocido por la Entidad Cliente y por el Firmante (actualmente es su número de documento de identidad), y será verificado por parte de la plataforma contra la base de datos de la Entidad Cliente.

5) La implementación en nuestra solución del botón "**He leído la documentación adjunta y consiento firmar el contrato**", da mayor robustez a la voluntad de firmar.

6) La **aceptación del proceso de contratación** por parte del Firmante se obtiene mediante la introducción de su **clave de firma OTP** enviada en el momento de la firma.

7) Los datos firmados quedan vinculados de forma única a la firma y al documento firmado por el usuario, de forma que no es posible la reutilización de la firma obtenida en otro documento diferente al contrato entregado, ya que, una vez obtenida la firma mediante la introducción de la clave de firma, el sistema emplea un doble sistema de seguridad encaminado a lograr garantizar la integridad de toda la información asociada a la firma en sí y al documento en general.

8) Además, la **Ley 34/2002 obliga a que la entidad emita confirmación de la recepción del contrato:**

- Mediante el envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente, o
- Mediante la confirmación documental de aceptación recibida por un medio equivalente al utilizado en el procedimiento de contratación, siempre que la confirmación pueda ser archivada por su destinatario.

En caso de nuestra plataforma de firma, dicho requisito se cumple al poner a disposición del firmante tanto la documentación firmada como todas las evidencias de la firma.

La aportación en juicio de las firmas electrónicas se regirá por las reglas generales de la prueba, y normalmente requerirá de la generación de un dictamen pericial, que en el caso objeto de este informe deberá ser emitido por parte de un perito informático especialista en seguridad.

En línea a todo lo anterior descrito, nuestro circuito de firma con OTP permitiría generar las evidencias suficientes para que, en caso de que se pusiera en duda la firma de un contrato, se puedan probar la identidad de los firmantes, así como el contenido del propio documento firmado generando el efecto jurídico de una firma electrónica avanzada.