

Identificación Electrónica y Servicios de Confianza

María GONZÁLEZ

Aasociada senior Information Techonology & Compliance de ECIJA. Asociada de ENATIC

Diario La Ley, Nº 8762, Sección Práctica Forense, 16 de Mayo de 2016, Editorial LA LEY

La cada vez mayor digitalización de los procesos de negocio y administrativos a través de la utilización de medios electrónicos y tecnológicos, acrecienta la necesidad de contar con mecanismos que permitan acreditar el origen e integridad de los datos comunicados, la identidad de los transmitentes, así como en su caso, manifestar su voluntad y consentimiento con respecto a la información transmitida, permitiendo a los mismos desplegar los correspondientes efectos jurídicos.

Normativa comentada

I. INTRODUCCIÓN

La cada vez mayor digitalización de los procesos de negocio y administrativos a través de la utilización de medios electrónicos y tecnológicos, acrecienta la necesidad de contar con mecanismos que permitan acreditar el origen e integridad de los datos comunicados, la identidad de los transmitentes, así como en su caso, manifestar su voluntad y consentimiento con respecto a la información transmitida, permitiendo a los mismos desplegar los correspondientes efectos jurídicos.

La acreditación de identidad, integridad, consentimiento y no repudio por medios electrónicos debe desplegar el mismo nivel de confianza que tradicionalmente ha tenido el soporte papel, debiendo disponer para ello de mecanismos y sistemas de identificación y firma electrónica que permitan acreditar y verificar dichos aspectos. Si añadimos además que nos encontramos en un mercado global, dichos mecanismos de identificación y firma electrónica, deben contar con el reconocimiento mutuo trasfronterizo, de forma que sea posible utilizar los documentos generados como prueba en procedimientos judiciales en todos los Estados miembro.

Con todos estos objetivos, se aprueba el Reglamento de Identificación Electrónica, (UE) 910/2014 (LA LEY 13356/2014) del Parlamento Europeo y del Consejo (en adelante eIDAS), que será de plena aplicación a partir próximo 1 de julio de 2016. Al tratarse de un Reglamento de carácter comunitario, se trata de una norma de aplicación directa a todos los Estados miembros, si bien, y de forma adicional, su aplicación va a suponer importantes cambios en la normativa nacional de firma electrónica establecida por la Ley de Firma Electrónica (59/2003, de 19 de diciembre), así como en la regulación específica de determinados servicios de confianza y en donde la Comisión ha delegado en los Estados la posibilidad de establecer condiciones específicas, siempre que dichas condiciones no vayan en contra u obstaculicen los objetivos del Reglamento, en concreto en relación con el reconocimiento mutuo y la interoperabilidad.

II. ¿CUÁLES SON LAS PRINCIPALES NOVEDADES INTRODUCIDAS POR EL EIDAS?

1. IDENTIDAD ELECTRÓNICA

Define el eIDAS la identificación electrónica como, «el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica» y que se llevará a cabo a través de los sistemas que sean notificados al efecto a la Comisión para el reconocimiento mutuo. Entiende el eIDAS por sistemas de identificación electrónica el «régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica».

El eIDAS hace referencia expresa a los diferentes niveles de seguridad que podrán tener los sistemas de identificación electrónica, y que permitirán la identificación y autenticación de los usuarios con unas garantías de seguridad diferentes, pero que permitirán adaptar dicho nivel de seguridad, al nivel de riesgo asociado al trámite, servicio o proceso que vaya a ser realizado por medios electrónicos.

2. SERVICIOS DE CONFIANZA CUALIFICADOS Y NO CUALIFICADOS

El eIDAS define los servicios de confianza como aquellos servicios electrónicos prestados habitualmente a cambio de una remuneración consistentes 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, o
- la creación, verificación y validación de certificados para autenticación de sitios web, o
- la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

Los prestadores de servicios de confianza podrán ser cualificados o no cualificados, siendo estos últimos aquellos prestadores que

que se halle instalado el certificado electrónico de forma local, aspecto que supone una de las principales novedades de la normativa de identificación electrónica y un verdadero impulso para la implantación y uso efectivo de los sistemas de identificación y firma electrónica por parte del conjunto de la sociedad (administraciones, entidades y ciudadanos).

El texto de la LFE, antes de la modificación operada por la Ley 25/2015, de 28 de julio (LA LEY 12418/2015), de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social (en adelante «LSO»), establecía que la firma electrónica reconocida o cualificada, debía cumplir con los siguientes requisitos:

- Permitir identificar al firmante.
- Permitir detectar cualquier cambio ulterior de los datos firmados.
- Estar vinculada al firmante de manera única y a los datos a que se refiere.
- Haber sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- Estar basada en un certificado reconocido.
- Ser generada mediante un dispositivo seguro de creación de firma.

La referencia expresa a «medios que el firmante puede mantener bajo su exclusivo control» limitaba el reconocimiento de la firma electrónica cualificada o reconocida en los sistemas de firma electrónica remota, al no cumplir este requisito de mantener bajo el exclusivo control del titular los datos de creación de firma, quedando sus efectos limitados a los establecidos para la firma electrónica avanzada.

Mediante la citada reforma introducida por la LSO, este requisito ha sido matizado, estableciéndose la posibilidad de que la firma electrónica sea creada por medios que el firmante puede utilizar, **con un alto nivel de confianza**, bajo su exclusivo control.

En este sentido, debemos tener en consideración que el eIDAS reconoce expresamente en su considerando 51 (LA LEY 13356/2014) que el firmante pueda poner a disposición de terceros, y confiar en estos, los dispositivos de creación de firma, del mismo modo que permite expresamente, e incluso promueve y promueve en su considerando 52 (LA LEY 13356/2014), la implantación y desarrollo de sistemas de creación de firmas electrónicas remotas, siempre que estos servicios sean gestionados por prestadores de servicios de confianza cualificados, realizándose bajo una condiciones de seguridad adecuadas.

En relación con la determinación de los requisitos de seguridad que deben cumplir todos los elementos que componen un sistema de identificación electrónica para prestar este tipo de servicios de firma remota, a través de la Decisión de Ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 (LA LEY 6106/2016) por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al art. 30.3 (LA LEY 13356/2014) y al art. 39 del eIDAS (LA LEY 13356/2014), la Comisión establece expresamente:

«En el momento de la adopción de la presente Decisión de la Comisión, varios prestadores de servicios de confianza ya ofrecen soluciones para gestionar los datos de creación de firma electrónica en nombre de sus clientes. Las certificaciones de productos se limitan actualmente a los módulos de seguridad de los equipos informáticos certificados con arreglo a diferentes normas, pero todavía no están certificados específicamente con arreglo a los requisitos aplicables a los dispositivos cualificados de creación de sellos y firmas. No obstante, no existen aún normas publicadas, como la norma EN 419 211 (aplicable a la firma electrónica creada en un entorno íntegramente gestionado, aunque no necesariamente de forma exclusiva, por el usuario), para un mercado igualmente importante de productos a distancia certificados. Dado que se están elaborando actualmente las normas que podrían ser adecuadas a tal fin, la Comisión completará la presente Decisión cuando esas normas estén disponibles y se consideren conformes a los requisitos establecidos en el anexo II del Reglamento (UE) n.º 910/2014 (LA LEY 13356/2014). Hasta el momento en que se establezca la lista de tales normas, puede utilizarse un proceso alternativo para evaluar la conformidad de esos productos en las condiciones previstas en el art. 30, apartado 3, letra b) (LA LEY 13356/2014), del Reglamento (UE) n.º 910/2014.»

En concreto, la definición de los requisitos técnicos que deberían cumplir los elementos del sistema utilizados para proveer un sistema de firma remota, que permita generar firmas electrónicas cualificadas, queda pendiente la estandarización de este aspecto, que ha quedado en manos del European Committee for Standardization (en adelante «CEN»), y que no tiene prevista la publicación de este estándar hasta bien entrado el año 2017, motivo por el cual la Comisión hace referencia a los procesos alternativos para la evaluación de conformidad de los dispositivos cualificados de creación de firma y sellos cualificados que vayan a utilizarse en entornos descentralizados.

5. OTROS SERVICIOS DE CONFIANZA PREVISTOS

El eIDAS regula de forma expresa otros servicios de confianza, como:

Sello de tiempo electrónico o «*datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante*».

Un sello cualificado de tiempo electrónico debe cumplir los requisitos establecidos por el art. 42 del eIDAS (LA LEY 13356/2014), es decir:

- Vincular la fecha y hora con los datos, de forma que se elimine razonablemente la posibilidad de modificar dichos datos sin que se detecte.
- Basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado, y
- haber sido firmada mediante el uso de una firma electrónica avanzada o sellada con un sello electrónico avanzado del prestador cualificado de servicios de confianza o por cualquier método equivalente.»

La utilización de sellos de tiempo electrónico, permite en el tráfico comercial y las relaciones con las Administraciones Públicas acreditar el momento exacto en el que se ha efectuado una determinada operación o proceso y la misma empieza a desplegar efectos jurídicos, aspectos con especial importancia y repercusión en cuestiones como:

∫ Aumento de la confianza en las operaciones y transacciones electrónicas. La inclusión de sellos de tiempo electrónicos en pedidos, facturas, contratos y otros documentos, garantizan que se han efectuado en un momento concreto, disminuyendo el riesgo de repudio y fraude.

∫ Protección de la propiedad intelectual, al permitir la acreditación del momento exacto en que se generó un determinado contenido (texto, imágenes, videos, sonido, etc), y en consecuencia, la prueba de que el mismo ha sido objeto, por ejemplo, de plagio.

∫ Ampliación de las funcionalidades de la firma electrónica, que al incluir un sello de tiempo electrónico permite tener evidencia del momento exacto en que un determinado documento ha sido objeto de firma, otorgándole medios adicionales para garantizar el no repudio.

Servicios de entrega electrónica certificada o «servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada».

Los servicios de entrega electrónica cualificadas deben cumplir los requisitos establecidos en el art. 44 del eIDAS, (LA LEY 13356/2014) es decir:

- Ser prestados por prestadores cualificados de servicios de confianza
- Asegurar con un alto nivel de fiabilidad la identificación del remitente
- Garantizar la identificación del destinatario antes de la entrega de los datos
- Estar protegidos el envío y recepción de datos por una firma electrónica avanzada o un sello avanzado de un prestador cualificado de servicios de confianza, de forma que se impida la posibilidad de que se modifiquen los datos sin que se detecte
- Indicar claramente al emisor y al destinatario de los datos cualquier modificación de los datos necesarios a efectos del envío o recepción de los datos
- Indicar mediante un sello cualificado de tiempo electrónico la fecha y la hora de envío, recepción y eventual modificación de los datos

Respecto de los servicios de entrega electrónica, y más en concreto, en relación con las comunicaciones y notificaciones certificadas, en España existe numerosa jurisprudencia previa al eIDAS que reconoce la validez de dichas comunicaciones y la acreditación mediante las mismas de aspectos claves como la integridad, autenticidad y no repudio, así como el momento exacto en el que las mismas fueron remitidas, recibidas e incluso leídas por el destinatario

Cabe señalar por su importancia el Auto Sala 1.ª T. Supremo 855/2010, donde el Tribunal Supremo reconoce el valor probatorio del correo electrónico certificado. En este caso, el requerimiento no había podido ser efectuado al cliente al resultar el mismo ilocalizable, por ello el procurador solicitó al Secretario Judicial de la Sala Primera para efectuar la notificación y requerimiento por vía telemática a través de un prestador de servicios de certificación privado. En este caso, reconoce el Tribunal el valor probatorio del correo electrónico certificado frente al correo electrónico normal. El auto del Supremo marca un antes y un después en la valoración judicial y en el uso de comunicaciones electrónicas certificadas, al explicitar la necesidad de que intermedie en la comunicación / notificación un prestador de servicios de confianza, en sintonía con lo establecido en el eIDAS, que permita garantizar la integridad de emisor, destinatario, mensaje, fecha y hora.

Servicios de autenticación de sitios web o certificado de autenticación de sitio web es definido por el eIDAS como una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado, dicha expedido por un prestador de servicios de confianza que cumpla los requisitos establecidos por su Anexo IV:

- Indicar que el certificado ha sido expedido como certificado cualificado de autenticación de sitios web
- Identificar al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo el Estado miembro en que dicho prestador está establecido y;
 - * en caso de persona jurídica, el nombre y número de registro oficial
 - * en caso de persona física, el nombre de la persona
- Identificar;
 - * para personas físicas, el nombre de la persona a la que se expida el certificado, o en caso de utilizar un seudónimo se indicara claramente
 - * para personas jurídicas, el nombre de la persona jurídica a la que se expida el certificado y cuando proceda el registro oficial

- Elementos de la dirección, ciudad y el Estado de la persona física o jurídica a quien se expida el certificado, y cuando proceda, el registro oficial
- Nombre o nombres de los dominios explotados por la persona física o jurídica a la que se expide el certificado
- Datos relativos al inicio y final del periodo de validez del certificado
- Código de identidad del certificado
- Firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor
- Lugar en que esté disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado
- Localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado.

6. DE LOS CERTIFICADOS DE PERSONA JURÍDICA A LOS SELLOS ELECTRÓNICOS

Los certificados de persona jurídica, son regulados en el art. 7 de la Ley de Firma Electrónica (LA LEY 1935/2003), estando su solicitud, emisión y custodia vinculada a las personas físicas administradoras, representantes legales o apoderados con poder bastante, pudiendo incluso establecer limitaciones por cuantía o materia, en cuanto a su utilización en las relaciones con las Administraciones Públicas o en la contratación de bienes o servicios. Sin embargo, el eIDAS no prevé ni regula los certificados de persona jurídica, ni la emisión de certificados de firma electrónica a personas jurídicas o entidades sin personalidad jurídica.

Así, el eIDAS, reserva únicamente a las personas jurídicas los denominados sellos electrónicos, que, según el considerando 59 del eIDAS (LA LEY 13356/2014), deben servir como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento. Del mismo modo, el considerando 65 (LA LEY 13356/2014) del eIDAS establece, que los sellos electrónicos, además de autenticar el documento expedido por la persona jurídica, pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, como programas informáticos o servidores.

Los prestadores de servicios que emitan sellos electrónicos deberán establecer las medidas que permitan poder acreditar la identidad de la persona física que representa a la persona jurídica; es decir, su emisión y utilización irá igualmente vinculada a la administración, representación legal o apoderamiento de las personas físicas vinculadas a la persona jurídica. Adicionalmente a los sellos electrónicos, el eIDAS prevé los certificados de persona física de representante, es decir, aquellos certificados electrónicos cualificados emitidos a favor de un representante autorizado de persona jurídica.

La problemática principal que se nos presenta a nivel nacional debido al no reconocimiento por el eIDAS de los certificados de persona jurídica, radica en que la utilización de dichos certificados está vinculada principalmente a la obligatoriedad establecida en el ámbito tributario, donde las personas jurídicas deben relacionarse con la Administración Tributaria exclusivamente por medios electrónicos, debiendo utilizar este tipo de certificados electrónicos reconocidos.

Para solventar esta situación, la Secretaría de Estado de las Telecomunicaciones y la Sociedad de la Información (SETSI) del Ministerio de Industria, emitió a finales del mes de enero de 2016 una nota informativa (<http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Documents/nota-web-certifs-pers-juridica.pdf>) acerca del futuro de los certificados de persona jurídica, estableciendo que antes del 1 de julio de 2016 dejarán de emitirse certificados de persona jurídica, pudiendo emitirse certificados de sello electrónico o certificados de persona física representante. Es decir, a partir de ese momento, los certificados de persona jurídica pasarán a relacionarse en la base de datos nacional y en la lista de confianza de prestadores de servicios de certificación, como certificados no reconocidos, si bien los certificados de persona jurídica emitidos antes del 1 de julio de 2016 podrán seguir utilizándose hasta la fecha de su caducidad o revocación.

(1) Ver, en su caso, el capítulo correspondiente a Protección de Datos y la comunicación de brechas de seguridad.

[Ver Texto](#)

(2) http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2015_235_R_0002&qid=1441792087678&from=ES

[Ver Texto](#)

Opinar (0)

QUEREMOS SABER TU OPINIÓN

Nombre

E-mail (no será publicado)

Comentario

Conozco y acepto las condiciones sobre protección de datos

Wolters Kluwer no se hace responsable de las opiniones vertidas en los comentarios. Los comentarios en esta página están moderados, no aparecerán inmediatamente en la página al ser enviados. Evita, por favor, las descalificaciones personales, los comentarios maleducados, los ataques directos o ridiculizaciones personales, o los calificativos insultantes de cualquier tipo, sean dirigidos al autor de la página o a cualquier otro comentarista.

Introduce el código que aparece en la imagen

Enviar

