1

LA FIRMA ELECTRÓNICA

1.1 RÉGIMEN JURÍDICO APLICABLE

La base legal de la firma electrónica está recogida en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y se desarrolla en más profundidad en la sección Base legal de las Firmas que retomaremos en el punto 1.3. *Tipos de firma*. La sección también explora, bajo que circunstancias la ley equipara la firma electrónica a la firma manuscrita, añade notas respecto a la normativa europea y hace distintas referencias legales a firmas con sellos de tiempo y avanzadas.

1.2 CONCEPTO

La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- Identificar al firmante de manera inequívoca.
- Asegurar la integridad del documento firmado (Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación).
- Asegurar el no repudio del documento firmado (Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento).

1.3 TIPOS DE FIRMA

Según la Ley 59/2003, se distinguen entre tres tipos de firma, recogidas en los artículos 3.1) 3.2) y 3.3):

- "*La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante*".
- "*La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control*".
- *"Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma"*.

Según el artículo 3.4) de la ley, la **firma electrónica reconocida** es la única que puede ser considerada equivalente a la firma manuscrita:

- "La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel".

1.4 USOS

La firma electrónica aporta tres características en la comunicación por Internet: **identificación del firmante, integridad de los datos y no repudio.**

Las aplicaciones prácticas de la firma electrónica son muchas y variadas, generalmente, orientadas a realizar operaciones por Internet que en la vida cotidiana requieren de una firma para validarlas.

Algunos ejemplos de operaciones que se pueden realizar actualmente haciendo uso de la firma digital son:

- Realización y presentación de la Declaración de la Renta a través de Internet.
- Presentación de documentación en los registros electrónicos administrativos.
- Petición y descarga on-line de la vida laboral.
- Recepción y firma de notificaciones electrónicas de las Administraciones.
- Firma de correos electrónicos.
- Firma de facturas electrónicas.

1.5 FORMATOS

Se denomina *formato de firma* a **como se genera el documento de firma** y como se guarda o estructura la información de firma en el documento generado.

La existencia de múltiples formatos de firma se debe a razones históricas, a como se ha ido introduciendo la firma en formatos de documentos ya existentes y a como se han ido añadiendo funcionalidades a lo largo del tiempo.

Según las necesidades o escenarios específicos puede interesar realizar la firma electrónica mediante los diferentes formatos existentes de firma existentes.

Existen **formatos básicos,** que aportan todos los elementos necesarios para crear una firma electrónica avanzada o reconocida:

- **XML Signature:** Es una especificación desarrollada bajo el amparo del *w3c* que permite la firma (completa o parcial) de documentos utilizando una notación XML estándar. XML Signature ofrece algunas ventajas frente a la firma tradicional ya que al estar basada en texto plano su estructura es legible por humanos. Funcionalmente, tiene mucho en común con PKCS#7, pero es más extensible y está orientada hacia la firma de documentos XML.

  Las firmas XML se pueden utilizar para firmar datos o recursos de cualquier tipo, normalmente documentos XML, pero cualquier cosa que sea accesible a través de una *URL* puede firmarse. Una firma XML que se utiliza para firmar un recurso fuera del documento XML que la contiene se llama una firma separada (**detached**), *figura 1.1*. Si se utiliza para firmar una parte del documento que la contiene, se llama una firma envuelta (**enveloped**). Si contiene los datos firmados dentro de sí mismo se llama una firma envolvente (**enveloping**).

```
<Signature Id=""MiFirmaDetached"" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
                    c14n-20010315"></CanonicalizationMethod>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
                sha1"></SignatureMethod>
        <Referente URI="http://www.ejemplo.org/midocumento.html">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/TR/2001/REC-
                        xml-c14n-20010315#WithComments"></Transform>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
                <DigestValue>vo7Aa…fwJ8=</DigestValue>
        </Reference>
    </SignedInfo>
    <SignatureValue>BwUwA…2OLtBQ=</SignatureValue>
    <KeyInfo>
        <X509Data>
            <X509Certificate>MIIB9jCC…wZgyg=</X509Certificate>
        </X509Data>
        <KeyValue>
            <RSAKeyValue>
                <Modulus>Pkk1…TP7U=</Modulus>
                <Exponent>AQAB</Exponent>
            </RSAKeyValue>
        </KeyValue>
    </KeyInfo>
</Signature>
```

Figura 1.1. XML Detached

- **PDF-Signature: es** una firma embebida en documentos PDF acordes a estándares ISO-32001. El que la firma embebida en un documento PDF hace que este formato sea el más "accesible". Es decir, una firma embebida en un PDF podría **ser visualizada por un usuario que disponga cualquier lector de PDF estándar**, como pudiera ser **Acrobat Reader**.

Icon	Status	Certificate and document status
	Certified & Valid	Certificate status: Valid. The signer used the certification process, and the signature was the first signature in the document. Document integrity status: the document has not changed since it was signed or has only changed in ways specifically permitted by the certifier.
	Valid	Certificate status: Valid. Document integrity status: the document has not changed since it was signed or only contains changes allowed by a previous signer, if any.
	Valid: Changed view	Certificate status: Valid. This icon may appear in a certified document, but it only appears on approval document signatures and not certification signatures. Document integrity status: the document has changed since it was signed. The current view of the document is not the same as that which was signed.
	Unknown	Certificate status: Unknown. The certificate has not been trusted (and is not untrusted), the revocation check could not complete, a chain could not be buit to trust anchor, and so on. Document integrity status: the document has changed since it was signed. The document the user is viewing is not the signed version.
	Unknown	Certificate status: Unknown. The certificate or any certificate in the chain up to the issuing root certificate has not been trusted (trust must exist for one certificate in the chain), the revocation check could not complete, a chain could not be built to trust anchor, the certificate has been trusted for signing but not for certifying. Document integrity status: the document has not changed since it was signed.
	Unknown	Certificate status: unverified. The certificate validation check has not executed ot could not complete due to bad revocation information, and non-responding server, no network connection, etc Document integrity status: unverified. The document integrity check has not executed or could not complete.
	Invalid	Certificate status: the signer´s certificate was invalid. Document integrity status: illegal changes have been made to the document

- **CMS (Cryptographic Message Syntax) / PKCS#7**: Formato binario usado para la firma, autenticación, resumen y encriptación de documentos. Fue diseñado, principalmente, para el intercambio de información a partir de correos electrónicos. Usa el estándar PKCS#7. Este formato además incorpora información de sellado de tiempo obtenidos por una TSA (Time Stamp Authority).

También existen **formatos avanzados:**

- **XAdES (Firma electrónica avanzada XML)**: Es una familia de firmas avanzadas, basadas en formatos XML. A diferencia que un formato embebido (como pudiera ser el PDF-Signature), es un lenguaje pensado para "conversar entre máquinas", es decir, el intercambio de información entre sistemas automatizados es el propósito de usar un formato basado en XML. Dentro de este formato de firmas, se han ido evolucionando distintas extensiones que dan respuesta a distintas necesidades y escenarios, las extensiones descritas a continuación no tienen que considerarse de menos a más en el grado de robustez, fiabilidad o seguridad, sino que deben considerarse como evoluciones del formato que dan respuesta a escenarios distintos, y no por ello compiten entre sí.
  - **XAdES-BES**: Firma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada.
  - **XAdES-EPES**. XAdES-BES al que se le incorpora información sobre la política de firma, como pudiera ser aquella información sobre el certificado empleado y la CA que lo emitió.
  - **XAdES-T (timestamp)**. Es un XAdES-EPES al que se le añade una segunda firma, pero en esta ocasión, una firma realizada por una TSA (Time Stamp Authority). Esta segunda firma aporta información específica sobre la fecha y hora exacta de la firma.
  - **XAdES-C (complete)**. Es un XAdES-T al que se le añaden referencias sobre los certificados y listas de revocación utilizadas para la validación del propio certificado utilizado para la firma. Por ejemplo: fue firmado por Certificado CCC emitidos por CA AAA y cuya CRL RRRR fue consultada en el momento de la validación.
  - **XAdES-X (extended)**. Es un XAdES-C al que se le añade información sobre la fecha y hora de los datos introducido para la extensión C.

- **XAdES-XL (extended long-term).**Es un XAdES-X al que se le incorporan los certificados (sólo clave pública) y las fuentes de validación que se usaron. A diferencia del C, donde sólo se incluía una referencia (un puntero), en este formato se embebe toda esa información. Por ejemplo, en el caso de una CRL, se incorpora la lista firmada de certificados revocados que fue consultada en ese momento. Esto se utiliza para garantizar la validación muchos años después de la firma incluso en el caso que la CA que emitió el certificado, o la fuente de validación (CRL) que se consultó, ya no esté disponibles (publicadas por ejemplo). Es decir, garantiza la validación off-line a largo plazo.
- **XAdES-A (archivado)**. Este formato incluye toda la información anterior pero incluye metainformación asociada a políticas de refirmado. Una política de refirmado establece un período de caducidad de la firma digital, y superado este tiempo, se procede a un refirmado. El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: hipotecas, títulos universitarios, escrituras, etc. 15, 20, 50 años, etc.

En el caso de firma de facturas electrónicas, en formato Facturae, el formato de firma es el XAdES.

- **PAdES (Firma electrónica avanzada en formato PDF):** Es un conjunto de restricciones y extensiones a PDF y al estándar ISO 32000-1 haciéndolo adecuado para la firma electrónica avanzada.

  Mientras que con PDF y el ISO 32000-1 se da un marco para firmar electrónicamente los documentos, la firma PAdES específica perfiles precisos para el uso de firmas electrónicas avanzadas bajo la Directiva de la Unión Europea 1999/93/EC**.**

  Un beneficio importante de PAdEs es que los documentos firmados electrónicamente permanecen válidos durante largos periodos de tiempo, incluso si los algoritmos criptográficos subyacentes están rotos.

  Los documentos firmados electrónicamente con formato PAdES pueden ser usados o archivados durante muchos años, incluso décadas, de manera que, en cualquier momento en el futuro, a pesar de los posibles avances tecnológicos, debe ser posible validar el documento para confirmar que la firma era válida en el momento en el que fue firmada, un concepto conocido como “Long-Term Validation” (LTV).

Para documentos en formato PDF, los datos de la firma se incorporan directamente en el documento PDF firmado, permitiendo que el contenido del archivo PDF sea copiado, almacenado y distribuido como un archivo electrónico simple. La firma también puede tener una representación visual como un campo de formulario, tal como podría tenerla en un documento impreso.

Una ventaja significativa del formato PAdES es que se despliega por medio de un software ampliamente reconocido como son los lectores PDF, es decir, no se requiere el desarrollo o la personalización de software especializado.

En la siguiente lista se definen brevemente los perfiles definidos por PAdES (ETSI TS 102 778):

- **PAdES Basic**. Perfil básico que cumple con los requisitos especificados en la norma ISO 32000-1.
- **PAdES-BES Profile (Enhaced).** Este perfil especifica una firma PDF avanzada basada en CAdES-bes e incorpora opción de incluir en la firma un sello de tiempo (CADES-T).
- **PAdES-EPES Profile (Enhaced)**. Este perfil especifica una firma PDF avanzada basada en CAdES-EPES. Es el PAdES-BES Profile añadiendole un identificador de política de firma y, opcionalmente, una referencia al tipo de compromiso adquirido.
- **PAdES-LTV Profile (Long Term).**Es el formato de firma longeva. Este perfil permite prorrogar por tiempo indefinido la validez de las firmas en formato PDF. Puede ser usado en conjunción con el PAdES-CMS, PAdES-BES o perfiles PADES-EPES. Este perfil es utilizado para garantizar la validación tras muchos años después de la realización de la firma. Es decir, garantiza la validación a largo plazo.

Es muy recomendable firmar documentos en formato PDF (formato de firma PAdES) pues el destinatario de la firma puede comprobar fácilmente, desde el mismo visualizador del PDF "Adobe Reader", la firma y el documento original firmado. Con otros formatos de firma esto no es posible si no se utilizan herramientas externas.

- **CAdES (Firma electrónica avanzada CMS Advanced Electronic Signatures)**: Es un conjunto de extensiones de datos firmados con sintaxis de mensajes criptográficos (CMS)por lo que es adecuada para la firma electrónica avanzada.

Mientras el formato CMS es un CAdES-T (timestamp) marco general para firmar documentos digitalmente, tales como E-Mail (S / MIME) o PDF, CAdES especifica perfiles precisos de datos firmados con CMS para su uso con firma electrónica avanzada en el marco de la Directiva Europea 1999/93/CE.

Un beneficio importante del formato CAdES es que los documentos firmados electrónicamente pueden seguir siendo válidos durante largos períodos, incluso si los algoritmos criptográficos subyacentes se rompen.

El principal documento que describe este formato es el ETSI TS 101 733 Firma Electrónica e Infraestructura (ESI) – CMS Advanced Electronic Signature (CAdES).

El formato CAdES tiene definidos 6 perfiles diferentes, según el nivel de protección ofrecido. Cada perfil incluye y mejora al anterior:

- **CAdES.** Forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada.
- **CAdES-T (timestamp).** Se le incorpora información el campo con sello de tiempos para proteger los datos de un posible repudio.
- **CAdES-C (complete).** Es un CAdES-T al que se le añade referencias sobre los certificados y listas de revocación utilizadas para permitir la validación off-line y su verificación en el futuro (sin almacenar los datos actuales de verificación).
- **CAdES-X (extended).** Es un CAdES-C al que se le añade información sobre la fecha y hora de los datos introducidos para la extensión C.
- **CAdES-X-L (extended long-term).**Es un CAdES-X al que se le incorporan los certificados (sólo clave pública) y las fuentes de validación que se usaron. Garantiza la validación off-line a largo plazo incluso si la fuente original no estuviera disponible.
- **CAdES-A (archivado).** Este formato incluye toda la información anterior pero incluye metainformación asociada a políticas de refirmado. Una política de refirmado establece un período de caducidad de la firma digital, y superado este tiempo, se procede a un refirmado. El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: hipotecas, títulos universitarios, escrituras, etc. 15, 20, 50 años, etc.

Podemos resumir los puntos a favor y en contra de estos certificados en el siguiente cuadro:

	A favor	En contra
CAdES	Todo tipo de formatos de fichero origen (Excel, Word, imágenes, etc.).	Receptor no siempre dispone de aplicación para visualización del fichero.
XAdES	Todo tipo de formatos de fichero origen (Excel, Word, imágenes, etc.).	Receptor no siempre dispone de aplicación para visualización del fichero. Generalmente orientado a ficheros XML.
PAdES	Visualización del fichero origen con cualquier visor de PDFs (son gratuitos). Acrobat Reader valida la firma.	Sólo admite PDFs.

En conclusión, un fichero de firma tiene un formato que viene determinado por estos aspectos:

- **Estructura del fichero**, formatos CAdES, XAdES, PAdES, OOXML, ODF, etc.
- **Dónde se guarda** el documento original.
- **Firmas de múltiples personas**.
- **Longevidad** de la firma y sello de tiempo.

Algunas aplicaciones de firma dejan elegir el formato a utilizar ("@ Firma"). Otras imponen siempre el mismo formato ("eCoFirma") y otras deciden automáticamente el formato en función del formato original del documento a firmar ("Firma Fácil").

1.6 DISPOSITIVOS DE FIRMA

1.6.1 Dispositivo seguro de creación de Firma

Es un instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Según el artículo 24 de la Ley 59/2003, de 19 de diciembre, de firma electrónica:

1. *"Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.*

2. *Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.*

3. *Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:*

   a) *Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.*

   b) *Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.*

   c) *Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.*

   d) *Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma".*

El artículo 25 recoge información sobre los dispositivos de creación de forma electrónica:

1. *"Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.*

2. *Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.*

3. *Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:*

   a) *Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.*

   b) *Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.*

   c) *Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.*

d) *Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.*

e) *Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.*

f) *Que pueda detectarse cualquier cambio relativo a su seguridad.*

4. *Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza".*

En el artículo 27, "Certificación de dispositivos seguros de creación de firma electrónica", nos indica que:

1. "*La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma.*

2. *La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.*

3. *En los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el Diario Oficial de la Unión Europea y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología que se publicarán en la dirección de Internet de este Ministerio.*

4. *Los certificados de conformidad de los dispositivos seguros de creación de firma serán modificados o, en su caso, revocados cuando se dejen de cumplir las condiciones establecidas para su obtención.*

   Los organismos de certificación asegurarán la difusión de las decisiones de revocación de certificados de dispositivos de creación de firma".

En resumen, es un instrumento hardware o software que sirve para aplicar los datos de creación de firma y que ofrece, al menos, las siguientes garantías: Que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

- Que exista seguridad razonable que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.
- Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.
- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste muestre al signatario antes del proceso de firma.

1.6.2 Dispositivo cualificado de creación de Firma

Es un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014:

1. "*Los dispositivos cualificados de creación de firma electrónica garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:*
   a) *Esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas.*
   b) *Los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica.*
   c) *Exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento.*
   d) *Los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.*

2. *Los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.*

3. *La generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante solo podrán correr a cargo de un prestador cualificado de servicios de confianza.*

4. *Sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:*

   a) *La seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales.*

   b) *El número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio".*

1.7 CERTIFICACIÓN DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN Y DISPOSITIVOS DE SERVICIOS DE FIRMA ELECTRÓNICA

En los artículos 26 a 28 de la Ley 59/2003 se recoge información relativa a la certificación de prestadores de servicios de certificación y dispositivos de servicios de firma electrónica:

En el artículo 26 se indica sobre certificación de prestadores de servicios de certificación que,

1. "*La certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.*

2. *La certificación de un prestador de servicios de certificación podrá ser solicitada por éste y podrá llevarse a cabo, entre otras, por entidades de certificación reconocidas por una entidad de acreditación designada de*

acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo.

3. *En los procedimientos de certificación podrán utilizarse normas técnicas u otros criterios de certificación adecuados. En caso de utilizarse normas técnicas, se emplearán preferentemente aquellas que gocen de amplio reconocimiento aprobadas por organismos de normalización europeos y, en su defecto, otras normas internacionales o españolas.*

4. *La certificación de un prestador de servicios de certificación no será necesaria para reconocer eficacia jurídica a una firma electrónica".*

En el artículo 27 se indica sobre certificación de dispositivos seguros de creación de firma electrónica que,

1. "*La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma.*

2. *La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.*

3. *En los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el Diario Oficial de la Unión Europea y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología que se publicarán en la dirección de Internet de este Ministerio.*

4. *Los certificados de conformidad de los dispositivos seguros de creación de firma serán modificados o, en su caso, revocados cuando se dejen de cumplir las condiciones establecidas para su obtención.*

   Los organismos de certificación asegurarán la difusión de las decisiones de revocación de certificados de dispositivos de creación de firma".

Por último, en el artículo 28, en relación al reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica,

1. *"Se presumirá que los productos de firma electrónica aludidos en el párrafo d) del apartado 1 del artículo 20 y en el apartado 3 del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el Diario Oficial de la Unión Europea.*

2. *Se reconocerá eficacia a los certificados de conformidad sobre dispositivos seguros de creación de firma que hayan sido otorgados por los organismos designados para ello en cualquier Estado miembro del Espacio Económico Europeo".*

1.8 LA FIRMA ELECTRÓNICA COMO MEDIO DE PRUEBA EN JUICIO

1.8.1 Valor probatorio de los documentos electrónicos

En este imparable proceso de digitalización en el que de manera irreversible e inmediata nos encontramos, y sobre todo tras la entrada en vigor de la reforma de, entre otras, de la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal (pretendiendo la incorporación del llamado expediente electrónico y regulando detalladamente las medidas de investigación criminal limitativas de los derechos reconocidos en el artículo 18 de la Constitución) adquiere especial relevancia el tratamiento en nuestro ordenamiento jurídico de las soportes electrónicos y su valor probatorio. Pretendemos poner de manifiesto con claridad, cuál es la eficacia probatoria de los distintos instrumentos informáticos que esta sociedad digital introduce, obviando las dificultades existentes en relación con la concreta definición de prueba electrónica. A fin de ser eminentemente prácticos, consideraremos prueba electrónica a cualquier soporte o documento informático, incluyendo los auditivos, ópticos o multimedia.

Las posibilidades de comunicación electrónica existentes son muchas y muy variadas, incluso cambiantes (ver artículo 299.2 LEC). La problemática que esta situación, ya no tan novedosa, genera es muy amplia y diversa y puede afectar, entre otros instrumentos, a ordenadores, dispositivos electrónicos, sistemas informáticos, instrumentos de almacenamiento de datos y bases de datos. Las comunicaciones habituales a través de Redes Sociales, correos electrónicos o teléfonos móviles ocasionan diariamente numerosos conflictos probatorios que

están dando lugar a una jurisprudencia no del todo uniforme. No obstante, lo cierto es que progresivamente el Derecho y la jurisprudencia, van aclarando y desarrollando criterios de interpretación cada vez más precisos, en consonancia también con la normativa europea más reciente, de la que es ejemplo el Reglamento (UE) nº 910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, que deroga la Directiva 1999/93/CE que en nuestro ordenamiento fue traspuesta mediante la vigente Ley 59/2003, de 19 de diciembre, de Firma Electrónica. También la jurisprudencia aporta cada vez con mayor frecuencia novedosas interpretaciones y, en este sentido, es un ejemplo el contenido de la reciente sentencia de 12 de enero de 2106, del Tribunal Europeo de Derechos Humanos, sobre las comunicaciones electrónicas en el ámbito laboral.

Se trata ahora de conocer en la práctica cuáles son los principios básicos que rigen en nuestro Derecho, y en nuestra jurisprudencia, en relación con el valor probatorio de las comunicaciones electrónicas, entendidas en el sentido amplio referido anteriormente, dentro del proceso judicial. Obviamente, nos referimos a la validez como medio de prueba de correos electrónicos, pantallazos, SMS, WhatsApp o cualquier otro sistema de mensajería instantánea, memorias USB, reproducciones en PDF, páginas web, etc.

Rigen los principios generales de aplicación para cualquier documento privado como medio de prueba (art. 326 LEC), aunque como veremos, existen especificidades propias de la naturaleza digital de estos soportes electrónicos: volatilidad, alterabilidad, vulnerabilidad, intangibilidad, etc.

1.8.2 Presupuestos generales a tener en cuenta

Hay que estar de manera primordial a lo dispuesto en la Ley de Enjuiciamiento Civil, por cuanto que con arreglo a su artículo 4, tiene carácter supletorio en todos los ámbitos jurisdiccionales (“En defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Ley”). El artículo 325 de la LEC remite al artículo 268 para conocer la forma de presentación de los documentos privados, y el criterio general es el de la presentación original o mediante copia autenticada por fedatario público, bastando copia simple del documento privado, siempre que no sea cuestionada por las demás partes. Asimismo, el importante artículo 326 de la LEC reconoce fuerza probatoria a los documentos privados, principio de prueba plena en el proceso, siempre que

su autenticidad no haya sido impugnada por la parte a quien perjudique. Si se produce la impugnación, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto. Si del cotejo o la prueba practicada no se dedujera la autenticidad del documento, el tribunal lo valorará conforme a las reglas de la sana crítica (artículo 334 de la LEC). En cualquier caso, hay que tener en cuenta lo dispuesto en el artículo 268,3 de la LEC, que exige, cuando el original del documento privado se encuentre en un expediente, protocolo, archivo o registro público, que se presente copia autentica o se designará el archivo, protocolo o registro", lo que hace que resulte más que conveniente designar ante cualquier comunicación electrónica, que por su propia naturaleza no se puede aportar en su soporte original, el elemento o equipo donde se encuentra, facilitando todos los datos necesarios para su identificación ante la eventualidad, previa impugnación, de tener que proceder a su análisis.

Por otro lado, no olvidar que resulta perfectamente posible la aportación al proceso como medio de prueba de cualquier instrumento de filmación, grabación y semejantes, como expresamente prevé, entre otros, el artículo 382 de la LEC, que se refiere a la reproducción de la palabra, el sonido y la imagen y de los instrumentos que permiten archivar y conocer datos relevantes para el proceso (Sección 8ª del capítulo VI del Título I del Libro II de la LEC). En general, resulta preferente la transcripción escrita de las palabras contenidas en este tipo de instrumentos, cuando sea posible, así como la aportación de los dictámenes y medios de prueba instrumentales que considere convenientes.

Resulta así especialmente importante saber como se aplican los criterios aludidos anteriormente a las diferentes comunicaciones electrónicas a las que nos estamos refiriendo a fin de garantizar los necesarios principios de integridad, autenticidad de origen, confidencialidad, licitud y no repudio (evitando pues la inseguridad, ante la falta de reconocimiento de la otra parte, que las posibilidades de manipulación existentes en el ámbito informático permiten). La aportación a un procedimiento de un correo o de cualquier otro tipo de soporte o documento electrónico, puede dar lugar a impugnar su autenticidad, es perfectamente posible generar digitalmente una supuesta comunicación inexistente e imprimirla en acreditación de la existencia supuestamente real de dicha comunicación o también a que se considere ilícita (artículo 287 LEC) la obtención de la comunicación, violando derechos fundamentales que afecten al secreto de las comunicaciones o al derecho a la intimidad.

En primer lugar, y en cuanto a la confidencialidad, la jurisprudencia ha dejado claro que una vez enviado, por ejemplo, un correo electrónico, ya no le pertenece al emisor en tanto que los transmite o dirige a un receptor y, por tanto, una vez finalizada la comunicación en sí misma, no hay secreto de comunicaciones (ámbito penal), lo que no quiere decir que por el contenido de la comunicación, ésta pudiera afectar hipotéticamente al derecho a la intimidad o a la propia imagen (ámbito civil). En cualquier caso, y dejando a salvo exigencias de deontología profesional de comunicaciones entre letrados, la existencia de un acto de comunicación permite en principio a cualquier de los intervinientes la aportación a un procedimiento judicial de dicha comunicación. La clave radica en la apertura por el receptor de la comunicación electrónica, aunque se plantean numerosas cuestiones que evidencian todavía distintos criterios según la jurisdicción en que nos desenvolvamos, evidenciando siempre la dificultades que la compleja realidad impone a las exigencias derivadas de los derechos de intimidad y del secreto de las comunicaciones (reenvíos, cadena de custodia, intervención de terceros, comunicación remota o presencial, etc.).

Otra cosa muy distinta es la "intervención de las comunicaciones", circunstancia que se da muy frecuentemente en el ámbito laboral cuando el empresario accede al contenido de los correos electrónicos de un trabajador sin su consentimiento. Aparece en este caso la doctrina de la "legítima expectativa de privacidad", que permite en definitiva la renuncia a la privacidad, incluso mediante Convenio Colectivo, cuando se utilizan ordenadores, herramientas o medios informáticos de titularidad empresarial (por ejemplo, dirección de correo electrónico corporativa). Sin embargo, en el ámbito penal en el que rige la garantía y protección del artículo 18.3 de la Constitución, no es posible reconocer eficacia probatoria a la intervención de las comunicaciones, aunque se trate de correo corporativo, por cuanto que resulta preceptiva la autorización judicial para la injerencia y, por tanto, en el procedimiento penal la aportación de comunicaciones sin intervención judicial suponen a priori una violación de derechos fundamentales conforme a lo dispuesto en el artículo 11.1 de la Ley Orgánica del Poder Judicial.

En segundo lugar, nos tenemos que referir de manera destacada a la firma electrónica y su eficacia probatoria. La firma electrónica, sea avanzada o no, tiene el efecto jurídico equivalente al de una firma manuscrita conforme a lo dispuesto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y en consonancia con el Reglamento de la UE nº 910/2014, de 23 de julio. Por tanto,

cualquier documento con firma electrónica resulta perfectamente admisible como prueba en los procedimientos judiciales, acreditando inicialmente la identidad del firmante e integridad del mensaje electrónico por él firmado, sin perjuicio de que otros medios de prueba puedan desvirtuar su validez. En este sentido, la Ley 34/2002, de 11 de julio, de Servicios en la Sociedad de la Información y el Correo Electrónico, reconoce con arreglo a lo dispuesto en el artículo 24.1, que si los contratos están firmados electrónicamente, se estará a lo dispuesto en la Ley de Firma Electrónica, aunque en otro caso, y en relación con la prueba de la celebración de los contratos suscritos en vía electrónica, se indica expresamente que se sujetará a las reglas generales del ordenamiento jurídico.

En tercer lugar, nos referiremos a continuación al modo en que han de aportarse a los procedimientos las comunicaciones digitales.

También debemos hacer mención al artículo 3.8 de la Ley 59/2003, que indica que *"el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.*

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil".

1.8.3 Como aportar a juicio las pruebas digitales

Los documentos digitales han de aportarse en forma electrónica, este es su formato o medio original como documento electrónico que es: USB, CD, etc. indicando siempre el ordenador o servidor de dónde proceden en su caso. Al margen de lo anterior, conviene recordar que existe la posibilidad certificar electrónicamente por un prestador de servicios de certificación, entre otras comunicaciones, los emails, SMS o burofaxes, lo que garantiza la integridad y autenticidad de la comunicaciones certificada (así lo ha reconocido de modo ya consolidado el Tribunal Supremo, sobre todo a partir del auto dictado por la Sala Primera en el recurso 855/2010).

En cualquier caso, cualquier documento o comunicación electrónica: correo electrónico, WhatsApp, SMS, etc., debe aportarse al procedimiento como ya hemos dicho y siempre que sea posible, en soporte electrónico o copia digital. Además, de transcribir el texto en papel impreso donde conste, en su caso, la cabecera e incluso los mensajes encadenados a efectos de dar mayor verosimilitud. La acreditación de la autenticidad de un correo electrónico requiere conocer al menos los siguientes datos: el emisor, el equipo o servidor entrante y saliente, la fecha y hora de envío y recepción. De ahí, que resulte conveniente poner a disposición del órgano judicial estos datos, así como el equipo informático de donde procede la comunicación aportada, lo que permitiría su análisis si existiera impugnación (artículo 268 LEC). Se trata de aportar inicialmente, con independencia de la señalada posible impugnación de parte, más que indicios sobre la verificación de la identidad y realidad de un correo o comunicación electrónica.

Junto con los anteriores elementos, habrá que valorar la conveniencia de protocolizar notarialmente el mensaje o la comunicación electrónica o, incluso, acudir al Acta de Presencia notarial, que aunque no constituye en sí misma prueba indubitada de la realidad de la comunicación, sí dará fe y constatará la existencia en un determinado soporte de los datos esenciales de la comunicación (bandeja de entrada o carpeta electrónica, fecha de envío o recepción que figura, datos de emisor y receptor, número de teléfono móvil, texto de la comunicación, existencia del pantallazo, etc.). Resulta aquí importante distinguir entre la protocolización del medio de prueba impreso ya anteriormente por el interesado (el Notario hará constar la identidad, el documento entregado y la fecha en que lo recibe, pero no la correspondencia del documento entregado con el contenido de la comunicación electrónica de que se trata, email, página web, etc.) y acta de presencia a que se refiere el artículo 199 del Reglamento Notarial, en la que

el fedatario público protocoliza los documentos exhibidos al mismo tal y como resulten de su percepción. En cualquier caso, hay que tener en cuenta que el Notario no acredita la autenticidad, veracidad o autoría del documento o soporte exhibido o protocolizado.

Por último, aportar un dictamen pericial, supone introducir en el proceso un medio de prueba (artículos 335 y ss. LEC) que en este caso adquiere especial importancia debido a las características propias de la "prueba electrónica", permitiendo incorporar al procedimiento una cualificada forma de acreditar en principio los elementos esenciales de la comunicación electrónica aportada, así como la autenticidad de la misma, aunque obviamente pueda resultar impugnada y contradicha y, en definitiva, valorada con arreglo también a las normas de la sana crítica (artículo 348 LEC). De ahí que entendamos que resulta preferible utilizar los dictámenes periciales como auxiliares en relación con el resto de evidencias probatorias aportadas al proceso, entre las que también adquieren relevancia las testificales que puedan trasladar también al juzgador la convicción de la realidad del mensaje o la comunicación. Por supuesto, que también cabe la utilización, según los casos, del resto de los medios de prueba admitidos por nuestro derecho, como son el reconocimiento judicial o el interrogatorio de parte.

En resumen, hay que aportar la prueba en soporte documental impreso, además del soporte digital correspondiente, y junto a ello, y según la relevancia y el caso concreto que nos ocupe, acompañar todas las evidencias o corroboraciones que nos garanticen una justa y racional valoración de la autenticidad de la prueba aportada. Para ello, como hemos visto, resulta más que aconsejable acudir además a la protocolización notarial y al dictamen pericial informático, sin perjuicio de utilizar también, si es posible, la prueba de testigos, el interrogatorio de parte y, en último término, el reconocimiento judicial. De cualquier modo, insistimos en la necesidad de aportar todo tipo de evidencias (contraseñas utilizadas, números de teléfonos móviles, titularidad de los mismos, servidor y/o equipo informático, fotografías y pantallazos, oficios a compañías, etc.).

En definitiva, se trata de llevar al proceso todo tipo de evidencias que permitan trasladar al órgano judicial la necesaria convicción sobre la autenticidad de la prueba electrónica aportada. La dificultad para acreditar fehacientemente la autenticidad de la misma dificultad intrínseca a la naturaleza digital del soporte electrónico y ante la hipotética impugnación de la contraparte, requiere un especial esfuerzo probatorio que permita finalmente una racional y correcta aplicación de las consabidas reglas de la sana crítica.

1.9 DOCUMENTOS FIRMADOS ELECTRÓNICAMENTE

El proceso básico que se sigue para la firma electrónica es el siguiente:

- El usuario dispone de un documento electrónico (una hoja de cálculo, un pdf, una imagen, incluso un formulario en una página web) y de un certificado que le pertenece y le identifica.
- La aplicación o dispositivo digital utilizados para la firma realiza un resumen del documento. El resumen de un documento de gran tamaño puede llegar a ser tan solo de unas líneas. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.
- La aplicación utiliza la clave privada para codificar el resumen.
- La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.

El resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y de las claves del firmante. La firma electrónica, por tanto, es el mismo documento electrónico resultante.

Figura 1.2. Proceso de firma electrónica

Como verificar un documento firmado

Si recibimos un documento firmado nos interesa validar la firma, es decir, comprobar que los datos firmados se corresponden con los originales, que el certificado con el que se ha firmado es válido y que la estructura del fichero es correcta.

¿Como sabemos si una firma es válida?

Podemos comprobar la validez de la firma de un documento, ver quién es el firmante y el documento firmado en VALIDe.

1.10 SERVICIOS DE CERTIFICACIÓN

Con carácter previo a la aprobación del eIDAS, cada estado miembro emitía sus propios certificados digitales, que son los documentos electrónicos que sirven para identificar a las personas y a las empresas.

El problema era que la validez de estos certificados fuera de las fronteras del país de emisión no estaba garantizada, y dependía de la existencia de convenios

entre la entidad emisora del certificado y su contraparte (en este caso, cualquier otro estado de la UE).

Para lograr el objetivo del mercado único digital, este problema debía ser resuelto. Y de esta necesidad nace el Reglamento eIDAS, cuyas siglas corresponden a Electronic Identification and Authentication Services, para fijar un estándar de identificación electrónica para armonizar y volver seguras las transacciones online en toda Europa. Y para ello, el Reglamento se apoya en lo que se denominan los servicios electrónicos de confianza.

Por tanto, con el objetivo muy claro de eliminar las fronteras a las transacciones electrónicas en la UE y construir un clima de confianza, el eIDAS establece y regula a nivel europeo dos conceptos:

1. El de los servicios electrónicos de confianza.
2. El del prestador de esos servicios electrónicos de confianza (lo desarrollaremos en el siguiente punto).

Básicamente, los servicios electrónicos de confianza permiten comprobar la identidad de origen en Internet, y también la integridad de los mensajes que se intercambian a través de la Red. Son por tanto un elemento fundamental en la eliminación de las barreras al mercado digital, puesto que refuerzan la seguridad de la información y contribuyen a la generación de confianza (de ahí su nombre).

El artículo 3 del Reglamento eIDAS recoge la definición de los servicios electrónicos de confianza. En el subapartado 16 se establece que "servicio de confianza" es el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

1. "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
2. La creación, verificación y validación de certificados para la autenticación de sitios web, o
3. La preservación de firmas, sellos o certificados electrónicos relativos a estos servicios."

1.11 CONCEPTO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN SUJETO A LA LEY

Un prestador de servicios de certificación es una persona, física o jurídica, que expide certificados electrónicos o que presta otros servicios en relación con la firma electrónica.

Para ser un prestador cualificado de servicios electrónicos de confianza se deben prestar servicios electrónicos de confianza cualificados y se debe tener el reconocimiento como tal por parte de un organismo de supervisión

En España, como en el resto de los países de la Unión Europea, los prestadores de servicios de certificación (PSC) se regulan mediante el Reglamento eIDAS (910/2014) por el que se deroga la Directiva 1999/93/CE.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, establece en su artículo 30 que los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología (actual Ministerio de Asuntos Económicos y Transformación Digital), el inicio de su actividad, así como información relativa a los servicios que prestan y sus correspondientes certificaciones de calidad. Esta información deberá ser convenientemente actualizada por los prestadores de servicios de certificación y será objeto de publicación en la dirección de Internet del citado Ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

En España, en la página del Ministerio de Asuntos Económicos y Transformación Digital se puede consultar el listado de prestadores de servicios cualificados o no cualificados, tal y como establece el Reglamento:

Podremos filtrar para hacer búsquedas, bien por el nombre del prestador de servicios de confianza, bien por los servicios electrónicos de confianza cualificados que preste, bien por los servicios de expedición de certificados electrónicos cualificados de las Administraciones Públicas o por los servicios de expedición de certificados electrónicos cualificados conformes con el Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que transpone la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior (PSD2).

En cuanto a los servicios electrónicos de confianza cualificados, en el desplegable podemos encontrar las siguientes opciones:

- Servicio de expedición de certificados electrónicos cualificados de firma electrónica.
- Servicio de expedición de certificados electrónicos cualificados de sello electrónico.
- Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web.
- Servicio de expedición de sellos electrónicos cualificados en el tiempo.
- Servicio cualificado de entrega electrónica certificada.
- Servicio cualificado de validación de firmas electrónicas cualificadas.
- Servicio cualificado de validación de sellos electrónicos cualificados.
- Servicio cualificado de conservación de firmas electrónicas cualificadas.
- Servicio cualificado de conservación de sellos electrónicos cualificados.

Respecto a los servicios de expedición de certificados electrónicos cualificados de las Administraciones Públicas, en el desplegable podemos encontrar las siguientes opciones:

- Certificados electrónicos cualificados de Empleado Público.
- Certificados cualificados de Sede electrónica de la Administración Pública.
- Certificados cualificados de Sello electrónico de la Administración Pública.

Por último, según los servicios de expedición de certificados electrónicos cualificados conformes con el Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que transpone

la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior (PSD2), podemos filtrar por:

- Certificados cualificados de sello electrónico PSD2.
- Certificados cualificados de autenticación de sitios web PSD2.

Los prestadores cualificados de servicios electrónicos de confianza son los que, para expedir un certificado digital a una persona física o jurídica, deben verificar su identidad. El artículo 24.1 del Reglamento eIDAS indica que *"al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios electrónicos de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado"*.

Para verificar la identidad, los prestadores cualificados de servicios electrónicos de confianza pueden hacerlo directamente, o bien a través de un tercero de conformidad con el Derecho nacional.

El Reglamento eIDAS establece 4 maneras para verificar la identidad:

1. *"En presencia de la persona física o de un representante autorizado de la persona jurídica.*
2. *A distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado.*

   Estos medios de identificación electrónica deberán cumplir además con los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad sustancial o alto.
3. *Por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a) o b).*
4. *Utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad."*

En España, es la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, del Ministerio de Energía, Turismo y Agenda Digital el organismo de supervisión que se encarga de verificar que los prestadores de servicios

electrónicos de confianza cualificados cumplen con estos requisitos, y también con los requisitos que se establecen para los servicios electrónicos de confianza cualificados.

La legislación relacionada es la siguiente:

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que transpone la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior (PSD2).
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

1.12 INFRACCIONES Y SANCIONES

Los artículos 31 a 36 de la Ley 59/2003, de 19 de diciembre, recogen esta materia que transcribimos a continuación:

"*Artículo 31. Infracciones.*

1. *Las infracciones de los preceptos de esta ley se clasifican en muy graves, graves y leves.*

2. *Son infracciones muy graves:*

   a) *El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.*

   Lo dispuesto en este apartado no será de aplicación respecto al incumplimiento de la obligación de constitución de la garantía económica prevista en el apartado 2 del artículo 20.

b) *La expedición de certificados reconocidos sin realizar todas las comprobaciones previas señaladas en el artículo 12, cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.*

3. *Son infracciones graves:*

a) *El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, excepto de la obligación de constitución de la garantía prevista en el apartado 2 del artículo 20, cuando no constituya infracción muy grave.*

b) *La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica contemplada en el apartado 2 del artículo 20.*

c) *La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en el artículo 12, en los casos en que no constituya infracción muy grave.*

d) *El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones señaladas en el artículo 18, si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.*

e) *El incumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en el artículo 21 respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

f) *La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Ciencia y Tecnología en su función de inspección y control.*

g) *El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta ley.*

4. *Constituyen infracciones leves:*

   El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en el artículo 18 y el incumplimiento por los prestadores de servicios de certificación de las restantes obligaciones establecidas en esta Ley, cuando no constituya infracción grave o muy grave, con excepción de las obligaciones contenidas en el apartado 2 del artículo 30.

Artículo 32. Sanciones.

1. *Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:*

   a) *Por la comisión de infracciones muy graves, se impondrá al infractor multa de 150.001 a 600.000 euros.*

      La comisión de dos o más infracciones muy graves en el plazo de tres años, podrá dar lugar, en función de los criterios de graduación del artículo siguiente, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

   b) *Por la comisión de infracciones graves, se impondrá al infractor multa de 30.001 a 150.000 euros.*

   c) *Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 30.000 euros.*

2. *Las infracciones graves y muy graves podrán llevar aparejada, a costa del sancionado, la publicación de la resolución sancionadora en el "Boletín Oficial del Estado" y en dos periódicos de difusión nacional o en la página de inicio del sitio de internet del prestador y, en su caso, en el sitio de internet del Ministerio de Ciencia y Tecnología, una vez que aquella tenga carácter firme.*

   Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, el número de usuarios afectados y la gravedad del ilícito.

Artículo 33. Graduación de la cuantía de las sanciones.

La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta lo siguiente:

1. *La existencia de intencionalidad o reiteración.*
2. *La reincidencia, por comisión de infracciones de la misma naturaleza, sancionadas mediante resolución firme.*
3. *La naturaleza y cuantía de los perjuicios causados.*
4. *Plazo de tiempo durante el que se haya venido cometiendo la infracción*
5. *El beneficio que haya reportado al infractor la comisión de la infracción.*
6. *Volumen de la facturación a que afecte la infracción cometida.*

Artículo 34. Medidas provisionales.

1. *En los procedimientos sancionadores por infracciones graves o muy graves el Ministerio de Ciencia y Tecnología podrá adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.*

   En particular, podrán acordarse las siguientes:

   a) *Suspensión temporal de la actividad del prestador de servicios de certificación y, en su caso, cierre provisional de sus establecimientos.*
   b) *Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.*
   c) *Advertencia al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.*

   En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y a la protección de los datos personales, cuando éstos pudieran resultar afectados.

2. *En los supuestos de daños de excepcional gravedad en la seguridad de los sistemas empleados por el prestador de servicios de certificación que menoscaben seriamente la confianza de los usuarios en los servicios ofrecidos, el Ministerio de Ciencia y Tecnología podrá acordar la suspensión o pérdida de vigencia de los certificados afectados, incluso con carácter definitivo.*

3. *En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.*

4. *En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en este artículo podrán ser acordadas antes de la iniciación del expediente sancionador.*

   Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los 15 días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

   En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 35. Multa coercitiva.

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 36. Competencia y procedimiento sancionador.

1. *La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.*

   No obstante, el incumplimiento de las obligaciones establecidas en el artículo 17 será sancionado por la Agencia de Protección de Datos con arreglo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. *La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en sus normas de desarrollo".*