

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora Curso: -Profª (PhD) María Nieves de la Serna Bilbao

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

LECCIÓN 7: FIRMA ELECTRÓNICA

Elaborado por Prof. Dr. Carlos Galán Pascual (PhD)

Profesor Área Derecho Administrativo// Departamento de Derecho Público

Profesor Máster Universitario en Derecho Telecomunicaciones,

Protección de Datos, Audiovisual y Sociedad de la Información// Instituto

Pascual Madoz

Universidad Carlos III de Madrid

Agencia de Tecnología Legal, S.L.



Esta obra está bajo una [licencia de Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0 España](https://creativecommons.org/licenses/by-nc-sa/3.0/es/).



IV. LA IDENTIFICACIÓN Y LA FIRMA ELECTRÓNICA EN EL DERECHO DE LA UNIÓN EUROPEA

- 1. La necesaria armonización transfronteriza**
- 2. La Identificación Electrónica en el Derecho de la UE**
- 3. Los Servicios de Confianza**
- 4. Los certificados electrónicos derivados del Reglamento eIDAS**
- 5. La firma electrónica, el sello electrónico y el sello de tiempo electrónico derivados del Reglamento eIDAS y su eficacia jurídica**

IV. LA IDENTIFICACIÓN Y LA FIRMA ELECTRÓNICA EN EL DERECHO DE LA UNIÓN EUROPEA.

1 La necesaria armonización transfronteriza.

El contenido de la Directiva 1999/93/CE y su heterogénea transposición al ordenamiento de los Estados miembro provocaron que el originario deseo de una relación transfronteriza fluida y garantista entre personas y organizaciones no se materializara adecuadamente.

Efectivamente, la relación entre estados requiere en la mayoría de las ocasiones unos mecanismos fiables y homogéneos en materia de identificación y firma electrónicas. Por ejemplo, no es posible un desarrollo coherente de la contratación pública electrónica si las partes implicadas (poderes adjudicadores y licitadores, de cualquier estado de la UE) no disponen de medios de identificación y firma reconocidos asimismo por todos ellos.

Consciente de esta realidad, las instituciones de la Unión Europea han venido trabajando durante los últimos años en una regulación que, con carácter obligatorio para sus destinatarios europeos, señale de manera armonizada los mecanismos de identificación y firma que deberán ser aceptados por todos en sus relaciones transfronterizas.

Resultado de ello ha sido, como hemos señalado más arriba, el Reglamento (UE) 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 la que se deroga la Directiva 1999/93/CE, conocido como **Reglamento eIDAS**.

El Reglamento eIDAS persigue, por tanto, asegurar la interoperabilidad en la UE:

- De la **Identificación Electrónica** (de personas y entidades)
- De los **Servicios de Confianza** (entre ellos, la generación y expedición de certificados electrónicos y otros servicios de confianza).

Su condición jurídica (Reglamento Europeo) confiere al Reglamento eIDAS la potestad de ser **directamente aplicable** en los Estados miembro (desplazando, por ejemplo, a la Ley 59/2003, de firma electrónica).

El gráfico siguiente muestra un esquema de los servicios regulados por el Reglamento eIDAS.



Esquema de servicios regulados por el Reglamento eIDAS

Una nueva ley nacional de Servicios de Confianza, que al tiempo de redactar estás líneas permanece en borrador, regulará aquellos aspectos que el Reglamento eIDAS deja a la libre regulación de los Estados miembro.

2. La Identificación Electrónica en el Derecho de la UE.

Como hemos señalado, una de las razones que impulsaron a las instituciones europeas la publicación del Reglamento eIDAS fue el deseo de mantener los **principios del mercado interior**, evitando imponer restricciones a la prestación de servicios de confianza en el territorio de un Estado miembro por

un prestador de servicios de confianza establecido en otro Estado miembro por razones que entraran en los ámbitos cubiertos por tal norma, permitiendo la libre circulación en el mercado interior de los productos y servicios de confianza que se ajusten al citado Reglamento.

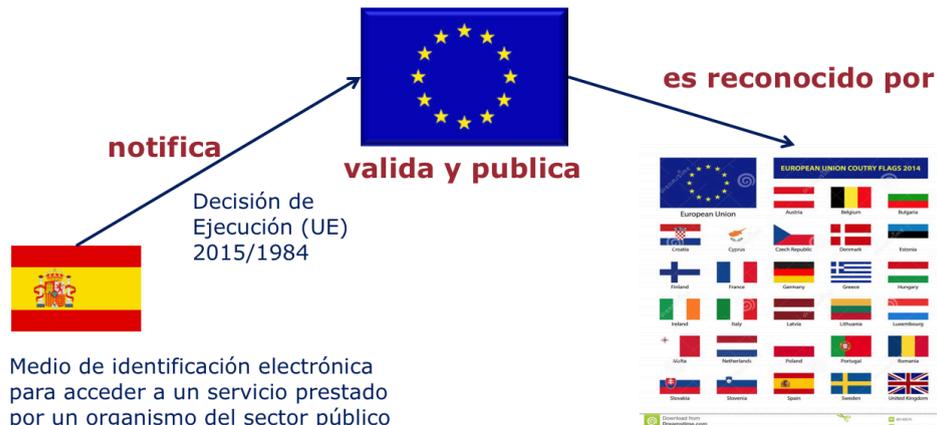
Estos principios relativos al mercado interior posibilitan y obligan al **reconocimiento mutuo de los medios de identificación electrónica** expedidos y **notificados** por los diferentes Estados miembro cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro, siempre que tal medio de identificación haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9 del Reglamento eIDAS; el nivel de seguridad de este medio de identificación electrónica corresponda a un **nivel de seguridad** igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto; y el organismo público en cuestión utilice un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea.

Como se muestra en el cuadro siguiente, el Reglamento eIDAS contempla tres **niveles de seguridad: Bajo, Sustancial y Alto**, atendiendo al grado de confianza de un medio de identificación en la identidad pretendida o declarada de una persona, niveles de seguridad regulados en el Reglamento de Ejecución (UE) 2015/1502.

Bajo	Se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad;
Sustancial	Se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad;
Alto	Se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial , y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, cuyo objetivo es evitar el uso indebido o alteración de la identidad.

Niveles de seguridad del eIDAS

El reconocimiento mutuo de los medios de identificación electrónica es obligatorio a partir del 29 de septiembre de 2018, debiendo los Estados fomentar el uso de los medios de identificación electrónica también en el sector privado.



Esquema del reconocimiento mutuo de los medios de identificación electrónica en la UE

3. Los Servicios de Confianza.

El aseguramiento transfronterizo de la firma electrónica exige que la UE establezca mecanismos a través de los cuales sus usuarios (firmantes emisores, por un lado, y receptores de documentos firmados, por otro) alcancen las debidas garantías respecto del procedimiento de firma usado, la identidad de los firmantes y la adecuada generación y expedición de los certificados digitales por los prestadores de tales servicios.

Esta necesidad ha obligado al Reglamento eIDAS a contemplar dos clases de servicios, el **Servicio de Confianza**, definido como: “El servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) 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 b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.”, y el **Servicio de Confianza Cualificado**, más exigente que el anterior y para el que

la UE contempla un especial control por parte de las entidades supervisoras de cada Estado miembro y de la propia UE.

Sea como fuere, el art. 19 del Reglamento eIDAS exige que los prestadores cualificados y no cualificados de servicios de confianza deberán adoptar las **medidas técnicas y organizativas** adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan, que eviten o reduzcan al mínimo el impacto de los incidentes de seguridad, informando al organismo de supervisión en un plazo no superior a 24 horas tras tener conocimiento y, en caso pertinente, a otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, la autoridad de protección de datos o, incluso, a los propios usuarios, de cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

La figura siguiente muestra este esquema de supervisión de los Prestadores de Servicios de Confianza.



Esquema de Supervisión de los Prestadores de Servicios de Confianza

Como hemos señalado, los **Prestadores de Servicios de Confianza Cualificados** sufren de un régimen de supervisión especial que implica que deberán ser auditados, al menos cada 24 meses, por un organismo de evaluación de la conformidad¹, confirmando que tanto los prestadores cualificados de servicios de confianza como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el Reglamento eIDAS.

A efectos de publicidad, cada Estado miembro establecerá, mantendrá y publicará **Listas de Confianza** con información relativa a los prestadores cualificados de servicios de confianza con respecto a los cuales sea responsable, junto con la información relacionada con los servicios de confianza cualificados prestados por cada uno de ellos².

Finalmente, aquellos Prestadores Cualificados de Servicios de Confianza que, habiendo superado el procedimiento de verificación de la conformidad señalado, hubieren sido incluidos en la correspondiente Lista de Confianza, podrán usar la **Etiqueta de Confianza «UE»** para indicar de manera simple, reconocible y clara los servicios de confianza cualificados que prestan.

En este sentido, la UE publicó el Reglamento de Ejecución (UE) 2015/806 de la Comisión, de 22 de mayo de 2015, por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados.

¹ En España, estos organismos o Entidades de Evaluación de la Conformidad han de ser previa y preceptivamente acreditados por la Entidad Nacional de Acreditación (ENAC) conforme al esquema de acreditación correspondiente.

² En España, esta Lista de Prestadores de Servicios de Confianza (TSL) se encuentra permanentemente actualizada y accesible en <https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx>



Etiqueta de confianza «UE» para servicios de confianza cualificados (en color)

En el ejercicio de sus competencias, y observándose un incumplimiento de alguno de los requisitos del Reglamento eIDAS, el organismo de supervisión (SESIAD, en España) podrá requerir a un prestador cualificado de servicios de confianza que corrija tales incumplimientos. Si este prestador no actúa en consecuencia en el plazo fijado, el organismo de supervisión, teniendo en cuenta el alcance, la duración y las consecuencias del incumplimiento, podrá retirar la cualificación al prestador o al servicio que este presta, procediendo a actualizar la correspondiente Lista de Confianza.

En la actualidad, los **servicios de confianza cualificados** regulados en el Reglamento eIDAS son los siguientes:

1. Servicio de expedición de certificados electrónicos cualificados de firma electrónica;
2. Servicio de expedición de certificados electrónicos cualificados de sello electrónico;
3. Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web;
4. Servicio de expedición de sellos electrónicos cualificados de tiempo;
5. Servicio cualificado de entrega electrónica certificada;
6. Servicio cualificado de validación de firmas electrónicas cualificadas;

7. Servicio cualificado de validación de sellos electrónicos cualificados;
8. Servicio cualificado de conservación de firmas electrónicas cualificadas;
9. Servicio cualificado de conservación de sellos electrónicos cualificados.

Servicios de confianza cualificados

4. Los certificados electrónicos derivados del Reglamento eIDAS.

Atendiendo a lo dispuesto en el Reglamento eIDAS, los **tipos de certificados** regulados son los que se muestran en el cuadro siguiente:

- Certificado de firma electrónica.
- Certificado **cualificado** de firma electrónica (Anexo I).

- Dispositivo de creación de firma electrónica.
- Dispositivo **cualificado** de creación de firma electrónica (Anexo II).

- Certificado de sello electrónico.
- Certificado **cualificado** de sello electrónico (Anexo III).

- Dispositivo de creación de sello electrónico.
- Dispositivo **cualificado** de creación de sello electrónico (Anexo II).

- Certificado de autenticación de sitio web.
- Certificado **cualificado** de autenticación de sitio web (Anexo IV).

Tipos de certificados previstos en el Reglamento eIDAS

Obsérvese que los certificados que gozan del carácter de “cualificados” se encuentran especialmente definidos y regulados en los Anexos del Reglamento eIDAS que se mencionan.

A título de ejemplo, reproducimos seguidamente parte de la tipología de certificados electrónicos expedidos por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM).

<p>Persona Física eIDAS</p>	<p>El Certificado FNMT de Persona Física, que se emite sin coste a cualquier ciudadano que esté en posesión de su DNI o NIE, es la certificación electrónica expedida por la FNMT-RCM que vincula a su Suscriptor con unos Datos de verificación de Firma y confirma su identidad personal.</p> <p>Este certificado le permitirá identificarse de forma telemática y firmar o cifrar documentos electrónicos.</p>
<p>Certificado de Representante eIDAS</p>	<p>Representante para Administradores únicos y solidarios:</p> <p>Certificado de Representante para administradores únicos y solidarios es la certificación electrónica expedida por la FNMT-RCM que vincula un Firmante con unos Datos de verificación de firma y confirma su identidad. El Firmante actúa en representación de una Persona jurídica en calidad de representante legal con su cargo de administrador único o solidario inscrito en el Registro Mercantil.</p> <p>Representante de Persona Jurídica:</p> <p>Certificado de Representante de Persona jurídica es la certificación electrónica expedida por la FNMT-RCM que vincula un Firmante a unos Datos de verificación de firma y confirma su identidad. Este certificado sustituye al tradicionalmente utilizado por las Administraciones Públicas para el ámbito tributario y que, posteriormente, se extendió para otros usos. Por tanto, este certificado se expide a las Personas Jurídicas para su uso en sus relaciones con aquellas Administraciones Públicas, Entidades y Organismos Públicos, vinculados o dependientes de las mismas.</p> <p>Representante de Entidad sin Personalidad Jurídica:</p> <p>Certificado de Representante de Entidad sin personalidad jurídica es la certificación electrónica expedida por la FNMT-RCM a una Entidad sin personalidad jurídica que vincula un Firmante a unos Datos de verificación de firma y confirma su identidad</p>

	en los trámites tributarios y otros ámbitos admitidos por la legislación vigente.
Administración Pública eIDAS	<p>La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, regula los sistemas de identificación de las Administraciones Públicas, así como los sistemas de firma electrónica del personal al servicio de las Administraciones Públicas y de sello electrónico para la actuación administrativa automatizada.</p> <p>Si desea utilizar alguno de los sistemas previstos en la citada Ley 40/2015, y por tanto está interesado en que su Administración cuente con el correspondiente acuerdo con la FNMT-RCM para la provisión de los mismos, puede dirigir su consulta al Área Comercial CERES.</p>
Certificados de Componente eIDAS	La FNMT-RCM también emite certificados electrónicos para la identificación de servidores o aplicaciones informáticas heredando la confianza de la FNMT-RCM como Autoridad de Certificación. Dentro de esta categoría ponemos a su disposición certificados de servidor SSL, certificados wildcard, certificados de firma de código y certificados de sello de entidad.

Tipología de certificados expedidos por la FNMT-RCM

5. La firma electrónica, el sello electrónico y el sello de tiempo electrónico derivados del Reglamento eIDAS y su eficacia jurídica.

Como hemos señalado, el Reglamento eIDAS ha venido a alterar la regulación en materia de firma electrónica.

La nueva regulación europea define la **firma electrónica** de la siguiente manera:

firma electrónica	Datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar (art. 3.10).
firma electrónica avanzada	La firma electrónica que cumple los siguientes requisitos (art. 3.11): a) Estar vinculada al firmante de manera única; b) Permitir la identificación del firmante; c) Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y d) Estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
firma electrónica cualificada	Una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica (art. 3.12).

Tipos de firma electrónica

Desaparecido el concepto de “firma electrónica de las personas Jurídicas”, de controvertida andadura en nuestra doctrina, el Reglamento eIDAS introduce -en su sustitución, podría decirse, y de forma similar a la firma- el **sello electrónico**, que define como se muestra seguidamente:

sello electrónico	Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos (art. 3.25).
sello electrónico avanzado	Un sello electrónico que cumple los siguientes requisitos (art. 3.26):

	<ul style="list-style-type: none"> a) Estar vinculado al creador del sello de manera única; b) Permitir la identificación del creador del sello; c) Haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo, y d) Estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.
sello electrónico cualificado	Un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico (art. 3.27).

Tipos de sello electrónico

Concluimos este repaso a los conceptos fundamentales y su acomodo en el Reglamento eIDAS con los mecanismos para la estampación de evidencias en materia de tiempo. Nos encontramos así con el tradicional concepto de **sello de tiempo**, que esta norma europea define del siguiente modo:

sello de tiempo electrónico	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;
sello cualificado de tiempo electrónico	<p>Un sello de tiempo electrónico que cumple los siguientes requisitos (art. 3.34):</p> <ul style="list-style-type: none"> a) Vincular la fecha y hora con los datos de forma que se elimine razonablemente la

	<p>posibilidad de modificar los datos sin que se detecte;</p> <p>b) Basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado, y</p> <p>c) 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.</p>
--	--

Tipos de sello de tiempo electrónico

Este nuevo marco jurídico derivado del Reglamento eIDAS contiene, entre otras, tres precisiones en torno a los **efectos jurídicos de las firmas electrónicas**, a saber:

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.

En todo caso, corresponde a las legislaciones nacionales determinar los efectos jurídicos de las firmas electrónicas en los Estados miembros, salvo para los requisitos establecidos en el Reglamento eIDAS.

2. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.
3. Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros.

Eficacia jurídica de las firmas/sellos electrónicos

Por lo que respecta al **uso de firmas electrónicas/sellos electrónicos en los servicios públicos**, el Reglamento eIDAS hace las siguientes precisiones (arts. 27 y 37, respectivamente):

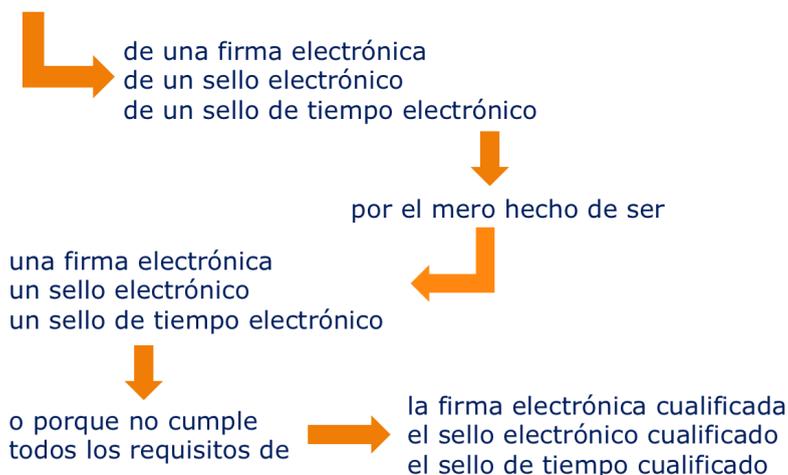
1. Si un Estado miembro requiere [una firma electrónica avanzada/un sello electrónico avanzado] con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho

Estado miembro reconocerá [las firmas electrónicas avanzadas/los sellos electrónicos avanzados], [las firmas electrónicas avanzadas basadas/los sellos electrónicos avanzados basados] en un certificado cualificado de [firma electrónica/sello electrónico] y [las firmas electrónicas cualificadas/los sellos electrónicos cualificados] por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en la norma³.

2. Si un Estado miembro requiere [una firma electrónica avanzada basada/un sello electrónico avanzado basado] en un certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá [las firmas electrónicas avanzadas basadas/los sellos electrónicos avanzados basados] en un certificado cualificado y [las firmas electrónicas cualificadas/los sellos electrónicos cualificados] por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en la norma.
3. Los Estados miembros no exigirán para la utilización transfronteriza de un servicio en línea ofrecido por un organismo del sector público [una firma electrónica/un sello electrónico] cuyo nivel de garantía de la seguridad sea superior al de [una firma electrónica cualificada/un sello electrónico cualificado].

La no denegación de los efectos jurídicos a las firmas electrónicas no cualificadas es igualmente predicable de los sellos electrónicos y a los sellos de tiempo electrónicos, como se muestra en el gráfico siguiente.

**No se denegarán
los efectos jurídicos**



³ Los actos de ejecución a los que se refiere el Reglamento eIDAS se concretan en la Decisión de Ejecución (UE) 2015/1506.