Entorno legal y normativo de la firma y sellos electrónicos

PID_00263146

Ignacio Alamillo i Domingo

Tiempo mínimo de dedicación recomendado: 5 horas

Universitat Oberta de Catalunya

Ignacio Alamillo i Domingo

Licenciado en Derecho y abogado del Ilustre Colegio de Reus, cuenta con el diploma de Estudios Avanzados en el programa de doctorado de Seguridad y prevención de la UAB, y es investigador del Centre de Govern del Risc de la Universidad Autónoma de Barcelona (GRISC UAB). Director general de Astrea La Infopista Jurídica y director de Innovación y CISO de Logalty (desde abril del 2009). Además, es vocal de tecnologías de la información de la Comisión Nacional de Acceso, Evaluación y Trial Documental. Ha sido consultor sénior en seguridad de la información, adscrito a la Dirección General de la Sociedad de la Información. Centro de Telecomunicaciones y Tecnologías de la Información. Generalitat de Cataluña. Director del Área de Asesoramiento e Investigación de la Agencia Catalana de Certificación y director del Área de Consultoría y Servicios Legales de la Agencia de Certificación Electrónica – ACE.

Índice

Introducción

Los documentos actúan como evidencias de la actividad diaria de las organizaciones. Estos documentos requieren estar dotados de una serie de características, como la autenticidad y la integridad. Estas características se conservan mediante una serie de actuaciones que veremos a lo largo del curso.

En este módulo en concreto vemos las particularidades de la firma de documentos en un entorno electrónico, bien sea presencial o a distancia, como viene sucediendo exitosamente en espacios como la administración electrónica o el comercio electrónico.

La principal normativa reguladora de estas instituciones la encontramos en el 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 (en adelante, Reglamento eIDAS).

El Reglamento eIDAS deroga la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (en adelante, la DFE) y desplaza la normativa española dictada en trasposición de la misma, la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, la LFE).

Este módulo está estructurado en tres bloques. En primer lugar, presentamos el concepto de firma electrónica, sus tipologías existentes, el régimen jurídico general y efectos jurídicos correspondientes a cada caso. Dichas nociones son significativas para comprender el funcionamiento y las garantías de los diferentes sistemas de firma electrónica a emplear en cada caso.

En segundo lugar, explicamos los certificados electrónicos, que soportan los sistemas de firma electrónica avanzada y reconocida, y que confirman la identidad del firmante.

En tercer lugar, presentaremos los servicios de confianza para la creación, validación y conservación de las firmas y sellos electrónicos, de especial relevancia para la práctica de gestión de documentos de archivo.

Objetivos

Los objetivos de este módulo son:

1. Conocer el marco legislativo de los documentos electrónicos en España, en concreto con el Reglamento europeo que rige la firma y el sello electrónico aplicado a los documentos electrónicos.

2. Conocer los sistemas de firma y sello electrónicos.

3. Familiarizarse con las normas técnicas que rigen la firma y el sello electrónicos.

4. Comprender el servicio de confianza de expedición de certificados de identidad personal y de sitios web.

5. Comprender el servicio de confianza de creación y validación de firma y sellos electrónicos.

6. Conocer el servicio de confianza de conservación de la firma y sello electrónicos.

1. Firma y sello electrónicos

En un entorno electrónico hemos de tener claro la diferenciación entre firma electrónica y sello electrónico. La firma electrónica se refiere solo a persona física. El sello electrónico se refiere a persona jurídica.

El Reglamento eIDAS, como anteriormente ya hicieran la DFE y la LFE, institucionaliza jurídicamente la firma electrónica, en un concepto que el Reglamento eIDAS reserva en exclusiva a la actuación de las personas físicas, así como el sello electrónico, reservado a la «actuación» de las personas jurídicas.

Como veremos, una de las principales diferencias entre ambas instituciones (firma y sello) va a ser precisamente el tipo de entidad usuaria de la misma –persona física para la firma, persona jurídica para el sello–; motivo por el cual procederemos a su estudio conjunto, sin perjuicio de ir anotando las diferencias relevantes entre ambas, que desde luego no son pocas.

El Reglamento eIDAS diferencia diversos tipos de firma/sello electrónico, siguiendo el mismo enfoque que anteriormente la DFE y la LFE. Como se verá, la firma/sello electrónico es un artefacto técnico que va a ser reconocido jurídicamente en función de una serie de propiedades que lo hacen relevante como fuente de prueba, al objeto de atribuir un documento a una persona y, en su caso, también identificar a dicha persona. Y, en este sentido, también hay que decir que la firma/sello electrónico no es un servicio de confianza, sino que es una institución que hace uso de los mismos, en algunos casos, como elemento de respaldo.

1.1. Tipos de firma electrónica y sello electrónico

Los tipos de firma y sello son las siguientes: ordinaria o simple, avanzada/o y cualificada/o. A continuación, vemos las diferencias entre ambos conceptos y sus implicaciones.

1.1.1. Firma y sello electrónico, en general

En este subapartado vemos los conceptos de firma y sello electrónicos ordinarios o simples, los sistemas y sus funciones.

Conceptos

El artículo 3.10 del Reglamento eIDAS define la **firma electrónica** como los «datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar».

Es una definición ligeramente diferente a la contenida originalmente en la DFE y en la LFE. Esta nueva definición refuerza el aspecto funcionalista de la definición, ya que lo importante será que los citados datos sean empleados precisamente para esta función de firmar, mientras que en la regulación anterior se hacía hincapié en el aspecto funcional de la firma como sistema, al menos, de identificación y autenticación electrónica.

En relación al **sello electrónico**, el artículo 3.25 del Reglamento eIDAS recoge la definición legal de sello electrónico, como los «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 los datos de estos últimos».

Por tanto, su utilidad viene dada por estos dos elementos (origen e integridad), que vienen referidos a los servicios de seguridad informática de autenticación del origen de los datos y de la integridad de los datos, presentados anteriormente. Esta definición es una novedad relevante en relación con la DFE y la LFE. Se trata de un mecanismo en cierto modo parecido a la firma electrónica, pero para que lo usen personas jurídicas. Así se deduce del Considerado 59 del Reglamento eIDAS, el cual indica que:

> «los sellos electrónicos 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».

Asimismo, de acuerdo con el Considerando 65:

> «además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores».

Por tanto, mientras que, en el caso de firma electrónica, el firmante es «una persona física que crea una firma electrónica» (artículo 3.9 del Reglamento eIDAS), en el caso del sello electrónico, el creador del sello es «una persona jurídica que crea un sello electrónico» (artículo 3.24 del Reglamento eIDAS).

Como se puede apreciar, una diferencia muy relevante entre ambos conceptos es que el de firma electrónica se construye por relación a la firma escrita, por lo que deberá poderse emplear una firma electrónica donde la legislación venga referida a una firma escrita –por lo que la firma electrónica se considera equivalente de la firma escrita–. Sin embargo, en el caso del sello electrónico no se aplica este enfoque, sino que se define para qué sirve el mismo, en lugar de referenciarse contra el empleo del «sello físico», del que muchas personas jurídicas disponen, y cuyo uso se encuentra regulado en gran cantidad de casos. Por ello, quizá se hubiera podido emplear también la técnica del equivalente funcional para la conceptualización jurídica de este mecanismo de seguridad informática.

Sistemas de firma electrónica

Los sistemas de firma electrónica actualmente disponibles en el mercado presentan una gran variedad, e incluyen desde dispositivos digitalizadores de firmas manuscritas hasta algoritmos de autenticación de mensajes basados en contraseñas. También se emplean algoritmos asimétricos, de firma digital, pero sin uso de certificados electrónicos, incluso en proyectos de ámbito europeo.

Por este motivo, con el nuevo concepto de firma electrónica, cualquier mecanismo técnico formado por datos asociados a otros datos que se emplee «para firmar» será admisible, incluso aunque el mismo no identifique/autentique de forma previa a la persona física, y sin perjuicio de que no todos éstos resultarán probatoriamente útiles.

Funciones de la firma electrónica

Respecto a qué significa la expresión «para firmar», se trata de una cuestión que se debe analizar conforme al derecho nacional, dado que el Reglamento eIDAS nada dice al respecto. En este sentido, resulta claro que la firma manuscrita cumple diversas funciones sociales típicas, normalmente institucionalizadas jurídicamente por la legislación o la jurisprudencia, por lo que cualquier tecnología que permita dicho cumplimiento deberá ser considerada como firma electrónica.

Desde este punto de vista, sucede que una de las funciones de la firma electrónica puede ser simplemente la atribución del mensaje a una persona identificada, pero sin que de la misma se desprenda la realización de declaración de voluntad alguna –así sucedería, por ejemplo, con la firma de una postal remitida a un familiar–; mientras que otra función socialmente típica será la prestación del consentimiento contractual, para la que se requerirán condiciones específicas a este respecto.

A diferencia de otros ordenamientos jurídicos, como el francés, en Derecho español no existe una definición de los requisitos que debería cumplir una firma manuscrita para la prestación del consentimiento contractual. No obstante, la jurisprudencia ha concretado algunas de estas características, para tener una referencia de los requisitos precisos para la tecnología aplicada a la firma electrónica. Un ejemplo es la sentencia del tribunal superior (STS) de 3 de noviembre de 1997, que ilustra los tres elementos que debe cumplir una tecnología para «servir para firmar». Estos elementos son:

- la identificación del firmante en condición de autor del documento
- la voluntad de obligarse
- la vinculación con el texto contenido en el documento, que presupone que el autor ha tenido acceso directo al mismo

De ello se desprende que la función social típica de la firma manuscrita sólo tiene sentido cuando la declaración de voluntad se emite en relación con un documento escrito, por lo que cualquier firma electrónica también se deberá proyectar sobre un soporte electrónico duradero que incorpore dicho escrito.

Ello no significa que sea imposible obtener una declaración de voluntad de una persona sin que exista un soporte escrito electrónico duradero, como sucedería en una contratación verbal registrada electrónicamente, pero en este caso no tendría sentido acudir a ninguna firma electrónica, igual que en el contrato verbal no se firma documento alguno en papel.

1.1.2. La firma y sello electrónicos avanzados

La segunda definición de firma y sello electrónicos tiene más requisitos que la simple firma y sello electrónicos. En este subapartado vemos los conceptos de firma y sello electrónicos avanzados, los datos de creación de firma, los dispositivos de creación y aplicación, datos de validación y tecnología garante de la integridad de los documentos firmados o sellados electrónicamente.

Conceptos y requisitos

Los artículos 3.11 y 3.26 del Reglamento eIDAS definen firma y sello electrónico avanzado. Veamos qué aspectos tenemos en cuenta cuando nos referimos a firma electrónica avanzada y sello electrónico avanzado:

1) Firma electrónica avanzada

El artículo 3.11 del Reglamento eIDAS define la **firma electrónica avanzada** como «la firma electrónica que cumple los requisitos contemplados en el artículo 26». Estos requisitos, citando textualmente, son los siguientes:

- estar vinculada al firmante de manera única;
- permitir la identificación del firmante;
- 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;
- estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Como se puede ver en su definición, la firma electrónica avanzada es técnicamente idónea para cumplir el fin social típico de la firma escrita a los que antes nos hemos referido, incluyendo la identificación del firmante en condición de autor del documento, la voluntad de obligarse y la vinculación con el texto contenido en el documento. Esto último, veremos que se basa en el uso de determinadas tecnologías.

2) Sello electrónico

De forma análoga, aunque no idéntica, a la firma electrónica avanzada, el artículo 3.26 del Reglamento eIDAS define el **sello electrónico avanzado** como «un sello electrónico que cumple los requisitos contemplados en el artículo 36». Estos requisitos, textualmente son los siguientes:

- estar vinculado al creador del sello de manera única;
- permitir la identificación del creador del sello;
- 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;
- estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Datos de creación de firma y sello

Como se puede ver de ambas definiciones, para la creación de la firma y sello electrónico avanzado se requiere del uso de unos datos de creación, que deberán ser objeto de diverso grado de control por parte de su titular.

Los datos de creación de firma electrónica son, de acuerdo con el artículo 3.13) del Reglamento eIDAS, «los datos únicos que utiliza el firmante para crear una firma electrónica». A estos datos se refería ya el artículo 24.1 de la LFE como «los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica», diferenciándose ambas definiciones en el enfoque más neutral que adopta el Reglamento.

El Reglamento eIDAS se refiere también a los datos de creación de sello electrónico como «los datos únicos que utiliza el creador del sello electrónico para crearlo», en su artículo 3.28.

En ambos casos, la creación de datos de la firma o del sello se trata del aspecto de mayor criticidad del sistema. Es un aspecto crítico porque la posesión o el acceso a los datos de creación de firma permite suplantar al firmante o creador del sello, respectivamente. Por tanto, los datos de creación de firma o sello han de poder ser protegidos contra la utilización indebida por terceros.

Esta protección tradicionalmente se había interpretado en el sentido de la exclusiva posesión de la clave únicamente por el firmante. Sin embargo, ahora, el Reglamento eIDAS considera un enfoque más amplio para adaptarse a nuevas opciones tecnológicas, incluso autorizando la gestión, por terceros, de los datos de creación, en determinadas condiciones; posibilidad que ha permitido la puesta en funcionamiento del sistema Cl@ve firma, con el DNI-e en la Nube.

Dispositivo de creación y aplicación

En este sentido, también es preciso aclarar que la creación de la firma o sello electrónico avanzado se produce empleando un dispositivo. Este dispositivo se define en el Reglamento eIDAS de la misma manera tanto para crear firma electrónica como sello electrónico. Concretamente, el artículo 3.22 del Reglamento eIDAS define el dispositivo como «un equipo o programa informático configurado que se utiliza para crear una firma electrónica». Del mismo modo, el artículo 3.31 del Reglamento eIDAS define el dispositivo de creación de sello electrónico como «un equipo o programa informático configurado que se utiliza para crear un sello electrónico».

Estas definiciones conectan la creación de la firma o sello electrónico con la aplicación (es decir, el uso) de los datos de creación de firma, de forma que el poseedor del dispositivo es realmente la persona que controla el proceso de creación de la firma o del sello, sea o no el suscriptor del certificado correspondiente.

Por este motivo, la firma o sello será imputable al firmante o creador del sello en la medida en que una persona no autorizada no pueda utilizar los datos de creación correspondientes. Ello justifica la necesidad de disponer del control del uso de los datos de activación de la firma o sello electrónico, al objeto de poder hacer esta imputación. Esto, como hemos visto, está previsto en la propia definición de firma o sello electrónico avanzado, aunque con la diferencia de que ese control deberá ser exclusivo en el caso de firma electrónica, y no en el caso del sello electrónico.

Datos de validación

Resulta también preciso referirse al artículo 3.40) del Reglamento eIDAS, que se refiere a los datos de validación de firma o sello electrónico, que define como «los datos utilizados para validar una firma electrónica o un sello electrónico», por parte de los terceros destinatarios de comunicaciones y documentos firmados.

Tecnología garante de la integridad

Esta segunda definición de firma y sello electrónico es incremental en requisitos sobre la más general de simple firma y sello electrónico. Exige que la tecnología permita identificar y atribuir unos datos a la persona que utiliza los mecanismos para producir la firma o sello. A diferencia de la firma manuscrita, la tecnología calificable como firma y sello electrónico avanzado debe garantizar la integridad del documento, de modo que las modificaciones posteriores del mismo sean detectables.

Como ya se ha avanzado, la definición se corresponde con las funciones tradicionalmente asignadas a la firma manuscrita, de modo que la firma electrónica avanzada resulta, con carácter general, un sistema más idóneo para que las personas físicas procedan a utilizar dicha tecnología en sustitución de la firma escrita.

De nuevo, se trata de una orientación que pretende resultar neutral desde una perspectiva técnica, permitiendo que diversas tecnologías reciban la calificación jurídica de firma y sello electrónico avanzado. A pesar de ello, el legislador comunitario claramente regula con una determinada tecnología en mente. Esta tecnología es la firma digital basada en criptografía de clave asimétrica, que, como además veremos, está basada en certificado electrónico; esto es, la

denominada PKI o infraestructura de clave pública. En este sentido, la neutralidad se encuentra más orientada a las diversas tecnologías de firma digital que a otras tecnologías diferentes.

En efecto, resulta más que evidente la equivalencia entre la clave privada (concepto técnico) y el dato de creación de firma o sello (concepto jurídico). También existe equivalencia entre la clave pública (concepto técnico) y el dato de validación de firma o sello (concepto jurídico), apoyando la equivalencia entre la firma digital (concepto técnico) y la firma electrónica avanzada o el sello electrónico avanzado (concepto jurídico).

Al menos desde una perspectiva puramente teórica, la firma y el sello electrónico avanzado puede, sin embargo, corresponderse con una firma digital, o no hacerlo, y en el primer caso, basarse en certificado, o no hacerlo, sin que ello afecte a su valor jurídico, pero siempre que se emplee una tecnología que permita el cumplimiento de todos los requisitos de la firma o sello electrónico avanzado, algo que no siempre es fácil.

Sucede también que, en el ámbito de la Administración electrónica, se ha venido admitiendo con carácter general la firma electrónica de los ciudadanos siempre que la misma se base en certificado cualificado admitido por la Administración. Es decir, la firma electrónica se ha configurado como un derecho del ciudadano en sus relaciones con la Administración, y sin perjuicio de que se hayan habilitado otros mecanismos de firma y sello electrónico. Por tanto, ciertamente se ha producido una fuerte promoción de una de las tecnologías de firma electrónica avanzada.

1.1.3. La firma y sello electrónicos cualificados

El tercer tipo de firma y sello electrónicos recogidos en el Reglamento eIDAS son los denominados «cualificados». Vamos a verlos a continuación.

Conceptos y requisitos

Las definiciones de firma y sello electrónicos están recogidas en el artículo 3.12 y 3.27 respectivamente. Vamos a verlos a continuación:

1) Firma electrónica cualificada

> El artículo 3.12 conceptúa la firma electrónica cualificada como «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».

Se trata, de nuevo, de una definición incremental en cuanto a los requisitos, que incorpora dos elementos adicionales a la firma electrónica avanzada:

- el dispositivo cualificado de creación de firmas electrónicas
- el certificado cualificado de firma electrónica

Este incremento de requisitos tiene como objetivo garantizar que la tecnología de firma electrónica reconocida o cualificada produzca su efecto típico; es decir, que sea idónea y adecuada para que una persona física se identifique y firme.

Nótese que tanto el dispositivo de firma como el certificado de firma deben ser cualificados, como medida de control previo que garantiza su idoneidad y, por tanto, que la firma electrónica cualificada efectivamente lo es.

De esta forma, el concepto de firma electrónica cualificada va a servir para denotar un subconjunto de tecnologías de firma electrónica como institución jurídica, a la que se asociarán efectos jurídicos específicos, «proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión», en palabras del Considerando (2) del Reglamento eIDAS.

Debe quedar claro, de todos modos, que no se debe considerar que una firma electrónica cualificada sea mejor ni más segura que otros tipos de firma, al menos técnicamente hablando. En realidad, lo que sucede es que se ha realizado una cierta apuesta, en cierto modo infringiendo el principio de neutralidad tecnológica, en favor de unas tecnologías concretas, lo cual sólo es aceptable porque la Ley sigue permitiendo, en régimen de no discriminación, otras tecnologías. Sólo de esta forma se explica que el sector privado haga un uso comparativamente mínimo de los sistemas de firma electrónica cualificada (como, por ejemplo, el DNI electrónico) en favor de otros mecanismos, como las contraseñas u, más recientemente, las firmas manuscritas digitalizadas, sin que se incrementen los niveles de fraude efectivo.

La firma electrónica cualificada y, en concreto, la que se encuentra sustentada en el DNI electrónico, constituye una línea de identificación y firma electrónica ofrecida por el Estado perfectamente razonable y defendible, y de la que las compañías privadas pueden hacer uso, pero sin renunciar a otras tecnologías idóneas en escenarios diversos, porque la realidad es que la base tecnológica que requiere el DNI electrónico (igual que otros sistemas de firma electrónica reconocida o cualificada) no se encuentra disponible en todos los escenarios, principalmente por cuestiones de interoperabilidad técnica.

Igualmente, la firma electrónica cualificada ha planteado problemas de usabilidad y de rechazo social en determinados procesos, por lo que el mercado sigue innovando y produciendo tecnologías seguras que, aun no gozando de una ventaja jurídica especial, resultan tanto o más seguras que la firma electrónica cualificada.

De esta conceptualización jurídica cabe criticar que la cualificación deba venir referida necesariamente estos dos elementos, porque supone una apuesta tecnológica que infringe el principio de neutralidad tecnológica; al contrario, la cualificación debería ser abstracta, porque de otro modo se discrimina la innovación; y ello sucede en la mayoría de servicios de confianza.

2) Sello electrónico cualificado

Por su parte, y de nuevo en una analogía clara con la firma electrónica cualificada, el artículo 3.27 del Reglamento eIDAS define el sello electrónico cualificado como «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»; de nuevo resultando aplicables las consideraciones realizadas en relación con la firma electrónica cualificada, pero para su uso por personas jurídicas.

Dispositivo cualificado de creación

Como hemos avanzado, uno de los elementos requeridos para obtener una firma o sello electrónicos cualificados –que como ya hemos visto es directamente equivalente a la firma escrita de la persona física, o directamente atribuible a la persona jurídica que lo genera, respectivamente– es el dispositivo cualificado de creación de dicha firma o sello. Vamos a analizar este dispositivo con algo de detalle.

Dicho dispositivo se define en el artículo 3.23) del Reglamento eIDAS, en relación con la firma electrónica, como «un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II». Respecto al sello electrónico, el artículo 3.32) del mismo Reglamento se refiere, en relación con el sello electrónico, a «un dispositivo de creación de sellos electrónicos que cumple mutatis mutandis los requisitos enumerados en el anexo II». De forma manifiestamente reiterativa, dispone el artículo 29.1 del Reglamento eIDAS, «[l]os dispositivos cualificados de creación de firmas electrónicas cumplirán los requisitos establecidos en el anexo II», previsión aplicable *mutatis mutandis* a los dispositivos cualificados de creación de sello electrónico en virtud de lo establecido en el artículo 39.1 del mismo Reglamento eIDAS.

En este sentido, por lo que respecta los dispositivos cualificados de firma electrónica, el Considerando (56) del Reglamento eIDAS indica que «en el presente Reglamento se establecen requisitos aplicables a los dispositivos cualificados

de creación de firmas electrónicas, a fin de garantizar la funcionalidad de las firmas electrónicas avanzadas», dando buena cuenta de la finalidad y orientación de dichos requisitos.

El Anexo II del Reglamento eIDAS, aplicable por tanto a dispositivos de creación de firma cualificados como a dispositivos de creación de sello cualificados, es el que realmente establece los requisitos que deben cumplir dichos productos, que en gran medida se refieren a los datos de creación de firma o sello, en diversas previsiones relevantes.

En primer lugar, el apartado 1.a) del Anexo II del Reglamento eIDAS exige que «esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica [o sello electrónico] utilizados para la creación de firmas electrónicas [o sellos electrónicos]», previsión completamente lógica, ya que, si estos datos de creación de firma o sello son conocidos por terceros, entonces dichos terceros pueden emplearlos para producir firmas en lugar de los legítimos firmantes.

En segundo lugar, el Anexo II del Reglamento eIDAS determina en su apartado 1.b) que los dispositivos cualificados han de garantizar que «los datos de creación de la firma electrónica [o sello electrónico] utilizados para la creación de una firma electrónica [o sello electrónico] solo puedan aparecer una vez en la práctica»; normativa que reconoce la imposibilidad de ofrecer esta garantía de forma absoluta, puesto que, en efecto, la garantía de unicidad del dato de creación se puede obtener de forma lo más aleatoria posible a partir de espacios numéricos muy grandes, pero incluso en este caso es difícil asegurar que dicho dato sea único, en especial cuando diversos prestadores generan datos de creación empleando mecanismos diversos.

En tercer lugar, el Anexo II del Reglamento eIDAS, aplicable tanto a la firma como al sello electrónico, determina en su apartado 1.c) que los dispositivos cualificados han de garantizar que:

> «exista la seguridad razonable de que los datos de creación de firma electrónica [o sello electrónico] utilizados para la creación de una firma electrónica [o sello electrónico] no pueden ser hallados por deducción».

Como se puede ver, la legislación no exige una seguridad absoluta o total, que difícilmente se podría garantizar, sin perjuicio de que el término «razonable» deba interpretarse a la luz de los potentes efectos jurídicos asociados a la firma o sello electrónicos cualificados, en especial a su efecto de equivalencia plena con la firma escrita o a su presunción de autenticidad, cuando se establezca.

Además, por su importancia, y como hemos avanzado, el dato de creación de firma y sello ha de ser convenientemente protegido por el firmante o creador del sello, habitualmente mediante el propio dispositivo de firma o sello electrónico, que por ello debe tener la consideración de cualificado, de acuerdo con el Reglamento eIDAS, o seguro, como lo denominaba la LFE.

En cuarto lugar, se contiene una referencia explícita a la protección de los datos de creación en el Anexo II del Reglamento eIDAS, aplicable tanto a dispositivos de creación de firma cualificados, como a dispositivos de creación de sello cualificados, cuando su apartado 1.d) dispone que los dispositivos deben garantizar que:

> «los datos de creación de la firma electrónica utilizados para la creación de una firma electrónica puedan ser protegidos por el firmante [o creador del sello] legítimo de forma fiable frente a su utilización por otros».

La formulación del Reglamento eIDAS es flexible, porque la referencia a la utilización de los medios de creación de firma/sello bajo control exclusivo se debe hacer con un alto nivel de confianza y, por tanto, no se exige un nivel absoluto o total de control. También resulta más acertado el uso del verbo *utilizar*, referido a dichos medios, puesto que denota correctamente la relación entre los medios de creación de firma/sello y la propia firma/sello, que es precisamente que los medios son el instrumento para la creación de la firma/sello, empleando los datos de creación.

Debido a este especial efecto de equivalencia, las especificaciones técnicas europeas desarrolladas para concretar los requisitos de los dispositivos seguros (o, ahora, cualificados) de creación de firma han adoptado una interpretación estricta del concepto de seguridad, que habitualmente conecta con el uso de un elemento de maquinaria o *hardware*, como por ejemplo un microchip criptográfico, para poder considerar el sistema como dispositivo cualificado de creación de firma electrónica.

1.2. Los efectos jurídicos de la firma y sello electrónicos

Hasta ahora hemos visto los conceptos y aspectos técnicos de la firma y sello electrónicos. Este apartado se centra en estos conceptos desde el punto de vista jurídico, partiendo del objetivo de la firma y el sello electrónicos. Recordemos que el objetivo es atribuir el contenido del documento a la persona que lo autoriza. Tomando en cuenta esto, vamos a estudiar los efectos jurídicos de la firma electrónica y del sello electrónicos, teniendo en cuenta su validez, la eficacia y el reconocimiento de los sistemas de firma y sello electrónicos.

1.2.1. La validez general de la firma y sello electrónicos

Llegados a este punto, no es conveniente seguir sin explicitar una cuestión importante: toda firma o sello electrónicos, con independencia de su calificación como «ordinarios» o «simples», «avanzados» o «cualificados» sirven al

mismo objetivo de atribuir el contenido del documento a la persona que lo autoriza y, por tanto, son legalmente válidos y, en función del caso, perfectamente aceptables.

En este sentido, hemos de tener en cuenta la validez de la firma y el sello electrónicos en todos los Estados miembros, y la no discriminación de la firma electrónica. Así, el Considerando (22) del Reglamento eIDAS dice que:

> «para contribuir al uso transfronterizo general de los servicios de confianza, debe ser posible utilizarlos como prueba en procedimientos judiciales en todos los Estados miembros».

Por su parte, el Considerando (49) del Reglamento eIDAS indica que:

> «el presente Reglamento debe establecer el principio de que no se deben denegar los efectos jurídicos de una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla todos los requisitos de la firma electrónica cualificada».

En definitiva, el Reglamento eIDAS instaura una norma jurídica de no discriminación de la firma electrónica diferente de la firma electrónica cualificada, que también se extiende al sello electrónico no cualificado. Los artículos a los que hace referencia son el 25.1 y el 35.1 respectivamente.

Así se muestra en el artículo 25.1 del Reglamento eIDAS, cuando establece que:

> «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».

A su vez, en relación con el sello electrónico, el artículo 35.1 del Reglamento eIDAS indica que:

> «no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado».

Consecuencia de todo ello es que debemos partir de la validez, *a limine*, de toda tecnología de firma y sello electrónicos, porque lo relevante jurídicamente es poder atribuir, desde la perspectiva de la prueba, un contenido a una persona física o jurídica, de acuerdo con las circunstancias concretas del caso, con una situación concreta que varía en función de las solemnidades y de las formas exigidas para la producción de cada acto jurídico –cuando sea el caso–. Cuestión diferente de la validez potencial será la de los efectos legales concretos de cada tipo de firma/sello, que queda en manos de cada legislador nacional.

Este régimen jurídico no ha resultado particularmente novedoso en España, dado que, como hemos visto, ya había sido el Tribunal Supremo español, nada menos que en Sentencia de 3 de diciembre de 1997, quien había indicado la perfecta admisibilidad de los sistemas de firma electrónica de todo tipo,

adelantándose en el tiempo a la aprobación de la primera legislación española sobre la materia, sin perjuicio de la conveniencia de elevar este principio (de no discriminación) a rango de ley formal.

En consecuencia, la diferencia real entre una simple firma o sello electrónicos, una firma o sello electrónicos avanzados o una firma o sello electrónicos reconocidos/cualificados no reside en su validez o admisibilidad jurídica, ni siquiera en su potencial eficacia, sino en el conjunto de requisitos técnicos necesarios para lograr o incluso garantizar jurídicamente unos efectos jurídicos concretos.

Finalmente, sucede que una firma o sello electrónicos (sean ordinarios, avanzados o incluso reconocidos o cualificados) pueden, a pesar de ser válidos, no ser idóneos, ellos solos, para atribuir todos los elementos de producción de un acto a una persona física o jurídica, de modo que necesitaremos elementos y condiciones adicionales para asegurar la evidencia que ofrece el documento en forma electrónica.

El documento electrónico

Por ejemplo, para obtener certeza de la existencia del documento electrónico –generalmente pocos momentos después de su producción y firma electrónica– podemos añadir a la firma o sello electrónicos un sello de fecha y hora criptográfico, obteniendo un valor probatorio del documento electrónico superior al documento privado en soporte papel.

1.2.2. La eficacia de la firma y sello electrónicos

Desde el punto de vista de la eficacia, por tanto, y respecto a la firma electrónica cualificada, el artículo 25.2 del Reglamento eIDAS establece que:

> «una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita».

Mientras que respecto al sello electrónico cualificado, el artículo 35.2 del Reglamento eIDAS determina que:

> «un sello electrónico cualificado disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado».

En ambos casos se trata de un efecto jurídico típico, que persigue la generación de seguridad jurídica para los usuarios de los sistemas de firma o sello electrónicos cualificados, que no deben regular el funcionamiento del sistema de firma o sello electrónico, ni obtener una previa autorización de los mismos, en sus relaciones con terceros.

Vamos a ver ahora en detalla la eficacia de la firma y los sellos electrónicos.

Firma electrónica

El artículo 25.2 del Reglamento eIDAS mantiene el enfoque, previsto en la normativa anterior, de determinar que el efecto jurídico típico de una firma electrónica cualificada será el equivalente al que tendría la firma manuscrita, por lo que se deberá poder emplear cuando una ley exija el requisito de firmar, al tiempo que el epígrafe 1 del propio artículo 25 prohíbe negar eficacia jurídica (potencial) a una firma electrónica que no sea cualificada.

Esta prohibición recogida en el epígrafe 1 del artículo 25 del eIDAS es muy significativa, y evita interpretaciones *sensu contrario* del efecto típico de las firmas electrónicas cualificadas, como las efectuadas en relación al artículo 3.4 de la LFE. Además, implica que ningún Estado miembro puede denegar todo efecto jurídico a una firma electrónica no cualificada, ni restringir su admisibilidad como prueba. Vamos a ver estos conceptos con más detalle.

Como hemos avanzado anteriormente, toda firma electrónica puede potencialmente recibir efectos jurídicos, no pudiendo ser ninguna tecnología discriminada por ser electrónica, algo que afectaría a la tutela judicial efectiva de forma evidente. Sin embargo, el legislador sólo define un efecto jurídico típico en relación con la firma electrónica cualificada –que es precisamente actuar como equivalente de la firma manuscrita–, permitiendo a los Estado miembros establecer los efectos jurídicos que consideren oportunos en relación con las firmas no cualificadas.

En su consecuencia, resultaría contrario a Derecho realizar una interpretación *a sensu contrario* del efecto típico de las firmas electrónicas cualificadas en perjuicio de las firmas no cualificadas. Esto es, no se puede considerar acertada la interpretación que se ha venido sustentando de que la firma electrónica no reconocida no tendrá el mismo valor que la firma manuscrita. Esto está basado en una visión excesivamente rigorista de la LFE, concretamente del artículo 3.4, que ha argumentado que si este artículo indica que «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], entonces la firma electrónica no reconocida no tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel, sino un valor diferente. De la misma forma, tampoco sería correcta la interpretación del artículo 25.2 del Reglamento eIDAS, si se considerase que la firma electrónica no cualificado no es equivalente a la firma manuscrita. Concretamente, partiendo del artículo 25.2 del Reglamento eIDAS que indica que «una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita»[2], sería erróneo que se considerase que una firma electrónica no cualificada no tendrá un efecto jurídico equivalente al de una firma manuscrita.

(1)Artículo 3.4 de la LFE.

(2)Artículo 25.2 del Reglamento eIDAS.

Y no es correcta esta interpretación porque la firma electrónica que no sea cualificada podrá obtener también efectos jurídicos, a tenor de la regla de no discriminación contenida en la DFE, la LFE y hoy en el Reglamento eIDAS.

Como hemos avanzado, los Estados miembros podrán establecer efectos jurídicos en relación con las firmas electrónicas no cualificadas, con carácter general o en relación a casos concretos, o incluso no establecer regla alguna al respecto –en cuyo caso nos encontraremos ante firmas electrónicas de efecto atípico. Sin embargo, los Estados miembros no podrán denegar todo efecto jurídico a una firma electrónica no cualificada, ni desde luego restringir su admisibilidad como prueba.

Ved también

En el subapartado 1.2.3. podéis consultar las reglas para la admisión transfronteriza de las firmas y sellos electrónicos.

Dado que la definición de firma electrónica contenida en el artículo 3.10) del Reglamento eIDAS se refiere a «los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar», todos los Estados miembros deben respetar que una firma electrónica no cualificada pueda potencialmente recibir el efecto de «servir para firmar». Esto es, una firma electrónica no cualificada puede potencialmente ser empleada en lugar de una firma manuscrita, porque en caso contrario estaríamos ante una infracción manifiesta del artículo 25.1 del Reglamento eIDAS.

Esta concepción doble se traduce en los niveles que caracterizan la eficacia de la firma electrónica, de acuerdo a dos reglas:

1) la regla jurídica de no discriminación, de acuerdo con la cual la parte a quien interesa la eficacia de una firma electrónica tiene derecho a que se practique una prueba suficiente, que determine si la firma electrónica era suficientemente fiable como para imputar el acto a la persona que la produjo;

2) la regla de equivalencia, que no elimina la necesidad de esta prueba que determine la fiabilidad de la firma, pero la reduce considerablemente, mediante la presunción de la especial idoneidad de determinada tecnología para actuar sustantivamente como si fuera la firma manuscrita de dicha persona, con eficacia *erga omnes*. Esta tecnología es la que se puede subsumir en el concepto jurídico de firma electrónica cualificada.

Mientras que la regla jurídica de no discriminación permite la existencia de firmas electrónicas atípicas, cuyos efectos sustantivos serán definidos por las partes, pudiendo «servir para firmar [en ese caso particular]», la regla de equivalencia establece una firma electrónica típica que aporta seguridad jurídica a las partes que deciden utilizarla, debido a su idoneidad para «servir para firmar [en todo caso]». Y dada la necesidad de admitir el empleo de firmas electrónicas no cualificadas en determinados ámbitos, se observa que en efecto los Estados miembros establecen efectos típicos singulares a dichas firmas no cualificadas, limitados a su jurisdicción.

Los Estados miembros no sólo pueden establecer efectos jurídicos con respecto a las firmas electrónicas no cualificadas, sino que también pueden hacerlo en relación con las firmas electrónicas cualificadas, siempre que dichos efectos vayan más allá del efecto típico definido en el Reglamento eIDAS, como por ejemplo sucederá en el caso del establecimiento de una presunción de autenticidad de la firma electrónica cualificada.

No se puede concluir esta sección sin indicar que ninguna firma electrónica puede emplearse en la absoluta totalidad de actuaciones personales, ya que el artículo 1.2 del Reglamento eIDAS, en línea de continuidad con la legislación anterior, aclara que el mismo «no afecta al Derecho nacional o de la Unión relacionada con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a la forma», por lo que nos podemos encontrar ante requisitos de forma que impidan el uso de la firma electrónica, incluso cuando la misma sea cualificada.

En efecto, resulta frecuente la exclusión de la posibilidad de emplear cualquier tipología de firma electrónica, incluida la firma electrónica cualificada, en determinados tipos de actuaciones jurídicas, por lo que hay que estar a lo que se determine conforme a la ley aplicable.

Sello electrónico

En el caso del sello electrónico vendría a suceder algo parecido de lo que hemos descrito de la firma electrónica, aunque con la diferencia de que no existe, como en la firma electrónica, un efecto de equivalencia descrito legalmente. Es decir, el efecto típico del sello es, como hemos visto, acreditar la autenticidad del origen de los datos y su integridad, y no ser equivalente a ninguna figura previamente existente, como pudiera ser el «sello físico de persona jurídica».

Dada la inexistencia de este efecto de «equivalencia con», se pueden generar dudas razonables acerca de los actos para los que se puede emplear un sello electrónico (con independencia de si el mismo es ordinario, avanzado o cualificado), excepto cuando nos encontremos ante el requisito legal, sustantivo, de que una persona jurídica deba ofrecer una garantía de autenticidad del origen de los datos y de la integridad del contenido, como sucede, por ejemplo, en el caso de las facturas electrónicas. Tampoco parece irrazonable acudir al empleo del sello electrónico en aquellos casos en que, como hemos visto anteriormente, exista una norma que prevea el uso de un sello (físico) de persona jurídica.

Sin embargo, aunque sabemos que para el Reglamento eIDAS el sello electrónico debe 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 – Considerando (59)– y para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores –Considerando (65)–, de ahí no se puede desprender que se pueda em-

plear para toda actuación jurídicamente vinculante para la persona jurídica, en especial a tenor de las normas de representación de los diferentes tipos de personas jurídicas.

Sorprende, a este respecto, que el Considerando (58) del Reglamento eIDAS establezca que «cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica», como si quisiera evitar que la existencia del sello pudiera afectar negativamente a la representación, en el sentido de discriminar negativamente la actuación del representante de la persona jurídica en cuestión.

Parece que para el legislador europeo un sello electrónico se pudiera emplear para toda actuación de una persona jurídica, pero hay que recordar que el Reglamento no afecta al Derecho nacional o de la Unión relacionado con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a la forma, por lo que se deberá acudir al caso concreto para dilucidar si se puede o no emplear un sello para una determinada actuación.

De nuevo, los Estados miembros pueden determinar en su legislación los efectos jurídicos que produzcan los sellos electrónicos. En este caso cabe prever que nos encontraremos ante dos tipos de normas:

1) las que podrán regular efectos de sellos electrónicos diferentes a los cualificados, para casos concretos

2) las que autoricen el uso del sello electrónico cualificado para determinadas actuaciones, –a diferencia de la firma electrónica cualificada

> Un ejemplo es el uso del sello electrónico en el ámbito de las relaciones entre las personas jurídicas y las entidades del sector público, en el funcionamiento electrónico del sector público, o en el caso de la factura electrónica.

En caso de que los Estados miembros no establezcan normas específicas relativas a los efectos de los sellos electrónicos, o de autorización de su uso en aquellos casos donde se requiera legalmente la representación, cabrá también atender a lo que las partes pacten, dentro de su ámbito de autorregulación, o a la utilidad intrínseca del sello, que por ejemplo se podría emplear para la autenticación de comunicaciones remitidas por personas jurídicas, a la acreditación de las actuaciones de acceso o de recepción, o quizá a la formalización de condiciones generales de la contratación.

1.2.3. El reconocimiento de los sistemas de firma y sello electrónico de los interesados de otros Estados miembros de la Unión Europea

Para completar la visión de los efectos jurídicos de las firmas y los sellos electrónicos, es preciso indicar que el Reglamento eIDAS ha establecido una serie de reglas para la admisión transfronteriza de las firmas y sellos electrónicos. Estas reglas van a afectar a la libertad de los Estados miembros de regular las condiciones de uso de estos sistemas de prueba electrónica en las relaciones que se establezcan con las mismas.

La idea es que cuando un Estado exija un sistema de firma o sello electrónicos el ciudadano pueda elegir el sistema, de acuerdo al apartado 5 de los artículos 27 y 37. El legislador quiere garantizar que se puedan emplear los sistemas de firma o sello electrónico avanzado de que dispongan los usuarios.

Reglas

Estas reglas se resumen en dos casos:

1) No exigir un nivel de seguridad superior para el uso transfronterizo en un servicio en línea ofrecido por un organismo del sector público[3].

2) Condiciones que deben cumplir los Estados miembros si se impone una firma o sello electrónicos avanzados, y que apuntan a normas técnicas y a la sintaxis informática de obligado cumplimiento[4].

(3)Artículos 27.3 y 37.3 del Reglamento eIDAS.

(4)Artículos 27.2 y 37.2 del Reglamento eIDAS.

Vamos a verlas en detalle a continuación:

1) Nivel de seguridad

En primer lugar, los artículos 27.3 y 37.3 del Reglamento eIDAS disponen, con carácter general, que los Estados miembros no exigirán, para el uso transfronterizo en un servicio en línea ofrecido por un organismo del sector público, una firma o sello electrónicos cuyo nivel de seguridad sea superior al de una firma o sello electrónico cualificados. Se trata de una norma claramente orientada a garantizar la actuación transfronteriza de los ciudadanos de la Unión, que en sus Estados de residencia típicamente van a obtener, a lo sumo, un sistema de firma o de sello electrónico cualificado. Sin perjuicio de lo que se acaba de indicar, como es lógico este régimen se aplica también a las firmas y sellos producidos por las entidades del sector público, que deban ser admitidos por las entidades de sector público de los restantes Estados miembros.

Firma o sello electrónico de nivel de seguridad superior al cualificado

Como ejemplo de una firma o sello electrónico de nivel de seguridad superior al cualificado, podemos citar la imposición obligatoria de un sello de tiempo electrónico cualificado sobre el contenido del documento firmado, o de un certificado de firma electrónica

con atributos –como en el caso de la representación legal o voluntaria– o de un certificado de atributos, adicional al certificado cualificado de firma electrónica.

Podemos considerar este aspecto como una reacción al régimen legal anterior, que como hemos visto permitía de forma expresa el establecimiento de condiciones adicionales al uso de la firma electrónica en las relaciones con el sector público.

2) Exigencia de firma

En segundo término, los artículos 27.2 y 37.2 del Reglamento eIDAS determinan que si un Estado miembro impone una firma o sello electrónicos avanzados 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 o los sellos electrónicos avanzados basados en un certificado y las firmas o sellos electrónicos cualificados por lo menos en los formatos o con los métodos contemplados en el apartado 5.

Por su parte, los artículos 27.1 y 37.1 del mismo Reglamento establecen que si un Estado miembro impone una firma o sello electrónicos avanzados 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 o sellos electrónicos avanzados, las firmas o sellos electrónicas avanzados basados en un certificado reconocido y las firmas o sellos electrónicos cualificados por lo menos en los formatos o con los métodos contemplados en el apartado 5.

Esta regla es muy conveniente porque existen potencialmente muchas y variadas tecnologías de firma o sello electrónico avanzado. Podría perfectamente suceder que los ciudadanos de un Estado dispusiesen de un sistema técnicamente incompatible con los sistemas de firma o sello electrónico avanzado de otros Estados. Gracias a esta norma, una persona que deba realizar una actuación transfronteriza para la que se imponga la firma o sello electrónico avanzado podrá acogerse al sistema que le ofrezca dicho Estado o emplear el sistema conforme a la norma técnica establecida por la Comisión. Para que ello sea posible, existen unas normas técnicas en las que se basa la sintaxis informática para facilitar las operaciones transfronterizas que deben cumplir las firmas o sellos electrónicos como vemos a continuación.

Normas técnicas

Como podemos ver, y ya hemos dicho, en los dos casos citados, lo que persigue el legislador europeo es, de nuevo, garantizar que se puedan emplear los sistemas de firma o sello electrónico avanzado de que dispongan los usuarios –aunque no de firma o sello electrónico ordinario, que quedaría excluido de admisión para usos transfronterizos – cuando un Estado miembro imponga la obligación de uso de éstos.

La idea es que cuando un Estado exija un sistema de firma o sello electrónico avanzado el ciudadano pueda elegir entre emplear dicho sistema, o alternativamente otros –y a su elección. Es decir, el ciudadano también puede emplear un sistema de firma o sello electrónico avanzado basado en certificado cualificado, o también un sistema de firma o sello electrónico cualificado. La condición es que el sistema elegido cumpla siempre con lo establecido en el apartado 5 de los artículos 27 y 37, que prevé la posibilidad de que la Comisión Europea establezca, mediante actos de ejecución, normas técnicas relativas a formatos de referencia o métodos alternativos, con base en instrumentos ya existentes.

Decisión 2011/130/UE

Un ejemplo de estos instrumentos es la Decisión 2011/130/UE, de 25 de febrero de 2011 por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior. Está Directiva ha sido modificada por la Decisión de Ejecución 2014/148/UE de la Comisión, de 17 de marzo de 2014.

Estas normas técnicas han sido adoptadas por la Decisión de Ejecución (UE) 2015/1506, que se refiere a los perfiles de base XAdES, CAdES, PAdES y con un contenedor con firma asociada (ASiC), definidos en las especificaciones técnicas ETSI TS 103 171 v.2.1.1, ETSI TS 103 173 v.2.2.1, ETSI TS 103 172 v.2.2.2 y ETSI TS 103 174 v.2.1.1, respectivamente; o al uso de métodos equivalentes descritos en la propia Decisión.

Decisión de Ejecución (UE) 2015/1506

Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

Los métodos equivalentes están previstos, en la Decisión, 2015/1506 para permitir la verificación transfronteriza de las firmas electrónicas –o los sellos electrónicos–, y exigen que «el Estado miembro en el que tenga su sede el proveedor de servicios de confianza utilizado por el firmante ofrezca a otros Estados miembros posibilidades de validación de firmas adecuadas, en la medida de lo posible, para el tratamiento automático»[5], como sucede, en España, con el servicio @firma.

(5)Artículo 2.1 de la Decisión.

Estas posibilidades de validación «parten de los requisitos para la validación de las firmas electrónicas y los sellos electrónicos cualificados a los que hacen referencia los artículos 32 y 40 del Reglamento (UE) Nº 910/2014».

El objetivo de la validación es «establecer requisitos comparables para la validación y para aumentar la confianza en las posibilidades de validación proporcionadas por los Estados miembros para otros formatos de firma electrónica o sello electrónico distintos de los comúnmente admitidos», según estable-

ce el Considerando (9) de la Decisión. Por ello aplicarán los requisitos de este proceso y su correlativo servicio de confianza, salvo excepción, normalmente referida a la exigencia del dispositivo cualificado de creación de firma o sello.

Hay que notar que, a diferencia de la previsión de los artículos 27.4 y 37.4 del Reglamento eIDAS, estas normas no presumen que la firma o sello sea efectivamente avanzado, sino que únicamente se refiere a la sintaxis informática que deben cumplir las firmas o sellos admisibles en operaciones transfronterizas, o los métodos equivalentes que resultan aceptables. Por ello, cabe indicar que se trata de una actuación que responde a la necesidad de circulación de las pruebas de atribución dimanante de la construcción del Mercado Único Digital.

Recordemos que la regla a la que nos hemos referido antes para operaciones transfronterizas es muy conveniente, ya que como sabemos existen potencialmente muchas y variadas tecnologías de firma o sello electrónico avanzado. Por ello, podría suceder que los ciudadanos de un Estado dispusiesen de un sistema técnicamente incompatible con los sistemas de firma o sello electrónico avanzado de otros Estados. Gracias a esta norma, una persona que deba realizar una actuación transfronteriza para la que se imponga la firma o sello electrónico avanzado podrá acogerse al sistema que le ofrezca dicho Estado o emplear el sistema conforme a la norma técnica establecida por la Comisión. Esto es, podría utilizar al menos un sistema de firmas o sellos basado en formato XAdES, CAdES o PAdES, en el nivel de conformidad B, T o LT, o los métodos equivalentes ya mencionados.

Sin embargo, es también preciso reconocer que la Decisión de Ejecución (UE) 2015/1506 se limita, en todo caso, a sistemas de firma y sello electrónico avanzado –o cualificado– respaldados por el uso de los correspondientes certificados cualificados. Por lo tanto, no desarrolla todas las posibilidades previstas en los artículos 27.1 y 37.1 dado que no se refiere a la firma y el sello electrónico avanzado que no se base en un certificado, lo cual no deja de ser una forma de inaplicar el mandato legal.

En efecto, conforme a la norma, si el Estado miembro exige firma electrónica avanzada debería admitir la firma electrónica avanzada, o la firma electrónica avanzada basada en certificado cualificado, o la firma cualificada, pero tras la aprobación de la Decisión de Ejecución (UE) 2015/1506 dicho Estado admitirá firma electrónica avanzada (normalmente a sus nacionales), pero podrá exigir (a los extranjeros) el uso de una firma electrónica avanzada basada en certificado cualificado o de una firma electrónica cualificada.

Por tanto, la regla de aceptación de cualquier formato que cumpla las normas técnicas es conveniente en términos de interoperabilidad, y puede considerarse razonable, frente a la dificultad de llegar a acuerdos sobre otros sistemas de firma o sello electrónico avanzado. No obstante, lo cierto es que esta regla supone un tratamiento diferente al previsto en el Reglamento eIDAS. Nada impide, sin embargo, que en el futuro se puedan incluir en la Decisión otros formatos de firma o sello electrónico avanzado que no se basen en certificados cualificados, o ni siquiera se basen en certificados, si ello resulta necesario.

2. El servicio de confianza de expedición de certificados de identidad personal y de sitios web

En este apartado nos vamos a referir a uno de los elementos que sustentan la acreditación electrónica y, por tanto, la prueba de la identidad, como es el certificado de clave pública, y el correspondiente servicio de confianza. Se trata de un instrumento que es diseñado y autorregulado con la función de identificación y autenticación, aunque posteriormente su uso se ha asociado más con la validez de la firma digital de documentos y comunicaciones electrónicas, especialmente desde la óptica de la normativa legal que procede a su institucionalización.

Sin embargo, lo cierto es que el certificado digital, y el servicio de confianza que lo sustenta, constituye una prueba electrónica de la identidad, sea de persona física o jurídica, y con independencia de si el certificado se emplea para avalar una firma electrónica, un sello electrónico o un nombre de dominio en Internet.

En este apartado vamos a ver la caracterización de los servicios de confianza, los requisitos que estos deben cumplir, y los efectos jurídicos del certificado electrónico.

2.1. Caracterización del servicio

Debemos, en primer lugar, caracterizar los certificados de firma y sello electrónico, objeto de este servicio de confianza, que la legislación regula como componente imprescindible de las modalidades más robustas de la firma y sello electrónico –avanzada y cualificada. Posteriormente, presentaremos los certificados de sitio web.

2.1.1. Certificados

De todos los tipos técnicos de certificados de clave pública que la autorregulación ha producido, el certificado cualificado de clave pública para la firma de las personas físicas ha sido el paradigma legal de certificado electrónico regulado, al cual se han acabado asimilando los restantes certificados de firma y sello electrónico, como ha sucedido en el caso de los certificados de sello electrónico para la actuación automatizada, administrativa o judicial.

Certificado de firma electrónica

El artículo 3.14) del Reglamento eIDAS se refiere al **certificado** de firma electrónica como «una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona».

Por su parte, el artículo 3.15) del mismo Reglamento, se refiere al **certificado cualificado** como un «certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I».

Certificado de sello electrónico

El artículo 3.29) define el **certificado** de sello electrónico como «una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona».

Por su parte, el artículo 3.30) se refiere al **certificado cualificado** como «un certificado de sellos electrónicos que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III».

Certificado de autenticación de sitio web

Por su parte, el artículo 3.38) del Reglamento eIDAS define el **certificado** de autenticación de sitio web 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».

Por otra parte, el artículo 3.29) de la misma norma define el **certificado cualificado** como «un certificado de autenticación de sitio web expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo IV».

2.1.2. Los certificados sustentan la identificación y la confianza

La identificación es la finalidad principal de los certificados. Esta identificación se expide en relación con diversos propósitos legales previstos en el Reglamento eIDAS, principalmente dos:

1) para respaldar la firma o el sello electrónico avanzado –a los que posteriormente nos referimos con detalle–, al confirmar la identidad de la persona correspondiente, y

2) para la autenticación de los sitios web; esto es, para que se pueda identificar a los citados sitios web en las conexiones realizadas con los mismos, o también desde los mismos.

Para sustentar la confianza de las partes usuarias, el Reglamento eIDAS establece un conjunto de normas mínimas referidas a dos aspectos:

1) contenido de cada uno de estos certificados

2) obligaciones mínimas de los prestadores que los expiden

Estas normas configuran, por tanto, los correspondientes servicios de confianza de expedición de certificados, tipificados en el Reglamento eIDAS.

La duda que se puede plantear, aunque sólo en relación con el uso de los certificados de firma electrónica o de sello electrónico, es si los mismos pueden utilizarse para que la persona física o jurídica identificada en el certificado pueda identificarse electrónicamente en un proceso que no exija la firma electrónica o el sello electrónico.

> Un ejemplo es el caso de acceso a una página web con contenidos informativos que requieran de la necesaria autenticación previa. Es decir, puede existir la duda de si estos certificados sirven, además de para firmar o sellar, para autenticarse, normalmente en un proceso de control de acceso. O, dicho de otra forma, si los mismos se pueden emplear en un servicio de autenticación de entidad.

Se trata de una duda que el Reglamento eIDAS no resuelve de forma directa, porque el mismo no es aplicable, como veremos, a las decisiones que tomen los Estados miembros en procesos domésticos de autenticación. Normalmente los procesos de autenticación se producen en el ámbito de la administración electrónica, aunque no de forma exclusiva. Por lo tanto, esta posibilidad de cursar un certificado para autenticarse dependerá de lo que establezca al respecto el derecho nacional. No obstante, lo que sí es seguro es el requisito de que un Estado podrá notificar el uso de certificados de firma o sello electrónico como sistema de identificación a efectos transfronterizos, en cuyo caso desde luego la respuesta será, por descontado, afirmativa.

A la vista de esta posibilidad, ciertamente parecería extraño que no se pudiera emplear un certificado cualificado de firma electrónica cualificada para cualquier otro proceso donde se requiera una identificación y autenticación electrónica, en su caso con base en la autonomía de la voluntad de las partes, sin perjuicio de la existencia de las excepciones legales que se encuentren debidamente justificadas.

Por otra parte, el Reglamento eIDAS no regula el uso de certificados electrónicos que no se puedan, al menos, emplear para validar firmas o sellos electrónicos, por lo que un certificado que se expida únicamente para identificarse –pero no para la creación de la firma o el sello electrónico– quedaría fuera de

la regulación armonizada, pudiendo ser, como ya sabemos, objeto de regulación en sede nacional, o funcionar simplemente en base a la autonomía de la voluntad de las partes, como sucede con otros sistemas de identificación electrónica.

2.1.3. Expedición de certificados

Los servicios de confianza correspondientes a la expedición de certificados (de firma electrónica, de sello electrónico y de autenticación de sitio web) deben cumplir los requisitos establecidos en el Reglamento eIDAS y, en su caso, en la legislación nacional, en especial los correspondientes a la modalidad cualificada del servicio.

Los servicios de confianza de expedición de certificados (exclusivamente de identificación), al encontrarse fuera del ámbito de aplicación del Reglamento eIDAS, quedarán sólo sujetos a la normativa nacional, pudiéndose incluso regular completamente en base a acuerdos de derecho privado. Todo ello sin perjuicio de que dicha normativa pueda imponer la aplicación de las normas generales aplicables a los servicios de confianza, o incluso las normas específicas del servicio cualificado de expedición de certificados.

Los prestadores que ofrezcan este servicio deben cumplir una serie de obligaciones:

- las obligaciones generales que se imponen a todos los prestadores de servicios de confianza

- las obligaciones exigibles a los prestadores cualificados de servicios de confianza

- las obligaciones correspondientes a los requisitos específicos del servicio

Antes de entrar en el análisis de los principales requisitos específicos de este servicio, conviene señalar la previsión legal contenida en los artículos 28.6, 38.6 y 45.2 del Reglamento eIDAS, en relación, respectivamente, con los certificados cualificados de firma electrónica, de sello electrónico y de autenticación de sitio web. En virtud de estos artículos, «la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados [...]», de modo que «[s]e presumirá el cumplimiento de los requisitos establecidos [...] cuando un certificado cualificado [...] se ajuste a dichas normas». Estos actos de ejecución «se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2», como hemos ya presentado anteriormente.

Existen diversas normas técnicas candidatas a ser establecidas a estos efectos, pero de momento la Comisión no ha ejercido su competencia. Esto resulta sorprendente por dos motivos. En primer lugar, por el esfuerzo y coste dedi-

cado a su desarrollo, bajo impulso por mandato de la propia Comisión durante los últimos dieciocho años –en especial, en virtud del importante mandato M/460. En segundo lugar, por el prestigio internacional manifestado en su adopción generalizada fuera de la Unión Europea.

Resultado de estos esfuerzos son las normas técnicas ETSI EN 319 411, partes 1 y 2, relativa a los requisitos de procedimiento y de seguridad para la expedición de certificados, y EN 319 412, partes 1 a 5, que se dedica a los perfiles (o plantillas) de certificados.

Estas normas, junto a las de sistemas fiables y a las de dispositivos de firma o sello, contienen los criterios que, incluso sin aprobación por la Comisión, se utilizan para la prestación del servicio, y que se emplean también para la evaluación de la conformidad requerida legalmente, por lo que suplen en gran medida la necesidad de un desarrollo legal nacional específico, a pesar de lo cual las normas nacionales vendrán en concretar determinados aspectos del Reglamento eIDAS.

2.2. Los requisitos del servicio

En este subapartado, veremos los requisitos que deben cumplir los prestadores de servicios de confianza teniendo en cuenta los siguientes tres aspectos:

1) los contenidos del certificado cualificado

2) la verificación de la identidad de la persona identificada en el certificado y, en su caso, del solicitante del certificado

3) la gestión del ciclo de vida del certificado cualificado

2.2.1. Los contenidos del certificado cualificado

Al objeto de cumplir con su función de identificación, los certificados deben, contener unas informaciones mínimas, que, en el caso del certificado cualificado, se encuentran legalmente determinadas, aunque la mayoría de ellas también deberán aparecer en los certificados sin cualificación.

El Reglamento eIDAS dedica a esta cuestión los siguientes artículos:

- el artículo 28.1, que refiere al Anexo I en relación con los certificados de firma electrónica

- el artículo 38.1, que refiere al Anexo III, relación con los certificados de sello electrónico

- el artículo 45.1, que refiere al Anexo IV, en relación a los certificados de autenticación de sitio web

En los tres tipos de certificados se prevén algunas informaciones comunes, incluyendo las siguientes:

1) Una **indicación** de que el certificado ha sido expedido como **certificado cualificado** (de firma, de sello o de autenticación de sitio web). El objetivo es cumplir con el necesario conocimiento que debe tener la parte usuaria de esta condición, a la que se asocian las garantías legales correspondientes. Esta indicación debe estar al menos en un formato adecuado para el procesamiento automático.

2) Los **datos de identidad del prestador** que expide el certificado, incluyendo su Estado de establecimiento.

3) Los datos de **identidad de la persona a la que se expide** el certificado; esto es:

a) El nombre de la persona física o un seudónimo, o de la persona jurídica y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales.

b) Sólo en el caso del certificado de autenticación de sitio web, los datos de identidad se completan con los siguientes elementos –atributos informativos, más correctamente:

- la dirección física, que incluye al menos la ciudad y el Estado
- la persona física o jurídica a quien se expida el certificado
- cuando proceda, según figure en los registros oficiales, el nombre o los nombres de dominio y la dirección electrónica, explotados por la persona física o jurídica a la que se expida el certificado

4) Los **datos de validación** de la firma o sello electrónico, o, aunque el Reglamento no lo explicite, la clave pública del sitio web, que son precisos para la ejecución de las operaciones técnicas que sustentan la prueba electrónica correspondiente.

5) Los **datos** relativos al inicio y final del **período de validez** del certificado. Se deben delimitar las fechas en que se pueden crear firmas o sellos –aunque la validación de las mismas podrá realizarse también transcurrido dicho periodo–, o confiar en autenticaciones del sitio web. Este periodo deberá establecerse conforme a lo que disponga el legislador nacional y, en todo caso, conforme a las normas criptográficas correspondientes.

6) El **código de identidad** del certificado, que debe ser único para el prestador cualificado de servicios de confianza, a los efectos de identificarlo unívocamente y diferenciarlo de cualquier otro certificado expedido por el mismo prestador.

7) La **firma electrónica avanzada** o el **sello electrónico avanzado del prestador de servicios de confianza expedidor** , a los efectos de proteger y autenticar el certificado, y permita a la parte usuaria confiar en que sus contenidos no han sido modificados.

8) El **lugar en que está disponible gratuitamente el certificado** que respalda la firma electrónica avanzada o el sello electrónico avanzado a que nos acabamos de referir. Esto es, se debe indicar la dirección de Internet en la que se puede recuperar el certificado expedido por la autoridad de certificación que, como vimos en la parte técnica, avala dicha firma o sello. Se trata de una novedad importante del Reglamento eIDAS en relación con la DFE y la LFE. Ello se explica por la necesidad que tiene la parte usuaria de acceder de forma efectiva a este certificado, a los efectos de poder verificar la correspondiente prueba electrónica.

9) La **localización de los servicios** que pueden utilizarse para **consultar el estado de validez del certificado cualificado**, de forma que la parte usuaria pueda determinar si puede confiar en las informaciones contenidas en el certificado. De nuevo, se trata de una importante novedad de Reglamento eIDAS respecto a la normativa anterior, que denota su importancia.

10) Finalmente, aunque sólo en el caso de los certificados de firma o sello, se debe indicar cuando los **datos de creación** relacionados con los datos de **validación** se encuentren en un **dispositivo cualificado de creación**. Esta información se debe indicar de forma adecuada, al menos en una forma apta para el procesamiento automático. Ello permite diferenciar entre un certificado cualificado de firma o sello cualificado –que incorpora esta indicación–, y un certificado de firma o sello avanzado, que no la incorpora. También es innovación del Reglamento eIDAS.

Es interesante hacer notar que en el Reglamento eIDAS ya no se incluya, entre los contenidos de los certificados, los relativos a los límites relativos a su uso, sean los mismos materiales o relativos a la cuantía. Estos contenidos sí se encontraban contemplados, con carácter opcional, en la DFE y la LFE, seguramente por los problemas de interoperabilidad, en especial semántica y jurídica, que los mismos han generado.

El Reglamento eIDAS ordena taxativamente, en su artículo 28.2, que:

> «[l]os certificados cualificados de firma electrónica no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo I».

De la misma forma hace con los certificados cualificados de sello electrónico, en el artículo 38.2. Esta prohibición no existe en el caso de los certificados de autenticación de sitio web, y posiblemente responde a la necesidad de corregir la práctica de los Estados miembros de exigir contenidos concretos a los certificados, con independencia del lugar de expedición de los mismos. Esto había tenido el efecto de impedir su uso en operaciones transfronterizas.

Esta prohibición se justifica en el Considerando (54) del Reglamento eIDAS, que indica que:

> «[l]a interoperabilidad y el reconocimiento transfronterizos de los certificados cualificados es un requisito previo para el reconocimiento transfronterizo de las firmas electrónicas cualificadas».

Por tanto:

> «los certificados cualificados no deben estar sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el presente Reglamento».

No obstante, establece como excepción, que:

> «en el plano nacional debe permitirse la inclusión de atributos específicos, por ejemplo identificadores únicos, en los certificados cualificados, a condición de que tales atributos específicos no comprometan la interoperabilidad y el reconocimiento transfronterizos de los certificados y las firmas electrónicas cualificados».

Además, conforme a los artículos 28.3 y 38.3 del Reglamento eIDAS, respectivamente en relación con los certificados cualificados de firma y sello electrónico, se establece que «[l]os certificados cualificados […] podrán incluir atributos específicos adicionales no obligatorios», los cuales tampoco «afectarán a la interoperabilidad y el reconocimiento de las firmas electrónicas cualificadas».

La regla general, por tanto, relativa a la prohibición de que los Estados miembros establezcan exigencias adicionales a los certificados cualificados se excepciona para permitir la imposición, por la normativa nacional, de atributos específicos obligatorios; y además se autoriza la posibilidad de inclusión voluntaria de otros atributos.

Nótese que esta regulación va a permitir que una normativa nacional pueda establecer prácticamente cualquier atributo adicional que se considere necesario en el marco de la prestación de los servicios de confianza, pero siempre con el límite de que no se afecte a la citada interoperabilidad y reconocimiento mutuo. Este límite implica que no se dicten normas nacionales que menoscaben los contenidos armonizados –aunque podrán detallarlos más, en especial en el marco de las normas técnicas que garantizan dicha interoperabilidad– y que los contenidos adicionales no impidan a partes usuarias establecidas en otros Estados miembros el uso del certificado cualificado en base a los contenidos armonizados, ignorando los atributos adicionales.

En todo caso, cualquier atributo –obligatorio o voluntario– que no haya sido objeto de armonización puede ser ignorado por la parte usuaria.

Certificado cualificado con poder de representación del firmante

Por ejemplo, en el caso de un certificado cualificado que incorpore el poder de representación del firmante, una parte usuaria podría adecuar su proceso de autenticación o de firma para hacer uso de dicha información, mientras que otra parte usuaria podría tratar el certificado como si el mismo no contuviera esta información. En ese ejemplo, para la primera parte usuaria el certificado es de persona física representante, y confía en el poder, y para la segunda parte usuaria el certificado es sólo de persona física, e ignora el poder.

Este régimen hace pensar que los atributos establecidos por la normativa nacional van a tener un reconocimiento limitado y preferentemente doméstico, debido a la falta de armonización de todos estos atributos en el nivel de la Unión Europea. Pero ello no significa que no puedan ser instrumentos útiles, como veremos sucede en el caso de los atributos extra previstos para las relaciones jurídico-administrativas.

Sin perjuicio de lo que se acaba de decir, y aunque el Reglamento no lo mencione, nada impide la aparición, en el nivel de la Unión Europea, de normativas que definan atributos que se impongan de forma obligatoria a determinadas personas, dado que el régimen contenida en los artículos 28.2 y 38.2 no afecta a las instituciones de la Unión, que lógicamente deberán actuar dentro de su ámbito de competencias.

2.2.2. La verificación de la identidad de la persona identificada en el certificado y, en su caso, del solicitante del certificado

La verificación de la identidad de la persona a la que se expedirá el certificado es uno de los requisitos más importantes a considerar, que ya se manifestaba en la normativa anterior. Esta verificación, por tanto, identificará la identidad de la persona en el certificado.

El Reglamento eIDAS contiene un novedoso régimen, en relación con la normativa anterior, en especial a la española, que conviene reseñar. Esta novedad es relativa a la verificación de la identidad de la persona a la que se expide certificados cualificados.

En concreto, el artículo 24.1 del Reglamento eIDAS ordena, de forma genérica, que un prestador cualificado verifique la identidad y cualquier atributo específico de la persona física o jurídica a la que se expide el certificado. Concretamente el artículo 24.1 detalla que:

«al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios 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».

Esta obligación es esencial dada la finalidad esencialmente identificativa del certificado, y cuya concreción se remite a lo que se establezca en el nivel nacional.

A pesar de ello, el mismo artículo dispone inmediatamente que «[l]a información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional» mediante alguna de las cuatro posibilidades que ofrece, y que constituyen una significativa novedad con respecto a la DFE. Esta indicación seguramente tiene como función evitar excesivas diferencias en las exigencias relativas a esta actuación del prestador, que inevitablemente se traducirían, por un lado, en barreras al reconocimiento transfronterizo de los certificados cualificados y, por conexión, de las firmas o sellos respaldados por los mismos, y por otro, en un menor nivel de confianza en los sitios web.

Se trata de posibilidades que recogen, a buen seguro, prácticas que se han ido generando en las diferentes leyes nacionales, y que ahora se recogen para toda la Unión. Sin embargo, no se ha recogido de forma plenamente armonizada, dada la remisión que en alguno de los casos se realiza a la normativa nacional correspondiente.

Vamos a analizar estas cuatro posibilidades que los prestadores de servicios de confianza utilizan para verificar la información relativa a la identidad: verificación en presencia de la persona o un representante, a distancia, por medio de firma o sello electrónico cualificados o mediante métodos reconocidos a escala nacional.

Verificación en presencia de la persona o un representante

En primer lugar, conforme al numeral a) del artículo 24.1 del Reglamento eIDAS, la verificación se podrá realizar «en presencia de la persona física o de un representante autorizado de la persona jurídica». Esta posibilidad ya se encontraba prevista en la LFE, en el artículo 12.a) y 13.1, con carácter previo a la expedición del certificado. Este artículo indicaba que:

> «[l]a identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho».

Esta norma se mantiene idéntica en el artículo 7.1 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

Se trata de la regla que en las normas técnicas se ha venido denominando «presencia física directa». Esta regla supone una barrera bastante clara a la extensión de la prestación de servicios desde un Estado miembro a potenciales clientes en toda la Unión, claramente derivada del coste de crear una red europea de oficinas propias o de colaboradores para esta tarea de verificación de la identidad. Por este motivo, en las normas técnicas se promovió el con-

cepto de la «presencia física indirecta», a partir de lo establecido en algunas normativas nacionales, proceso que parece haber cristalizado en las restantes posibilidades previstas en el artículo 24.1 del Reglamento eIDAS, que veremos a continuación.

Verificación a distancia

En efecto, la segunda posibilidad prevista en el numeral b) del artículo 24.1 es realizar dicha verificación «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, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad "sustancial" o "alto"». Esta posibilidad excluye el uso de estos medios de identificación cuando se hayan expedido sin la presencia personal de las citadas personas.

Se trata de un caso específico de uso de un medio de identificación para un uso privado, por previsión expresa del Reglamento eIDAS. Puede facilitar el desarrollo de la actividad de expedición de certificados en el Mercado Único Digital, al eliminar la necesidad de la presencia personal y autorizar al prestador a confiar en un subconjunto de los citados medios de identificación.

Uso de un medio de identificación para uso privado

Un ejemplo de esta posibilidad –seguramente el más relevante, y actualmente implementado por diversos prestadores españoles– es el uso del DNI electrónico o equivalente de otros Estados miembros, como la nPA alemana, que permitiría a un nacional alemán adquirir un certificado expedido en España, de convenirle, sin tener que desplazarse.

Verificación por medio de firma o sello electrónicos cualificados

En tercer lugar, el numeral c) del mismo artículo 24.1 autoriza que la verificación se realice «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)». Es una norma que tiene una lógica similar a la del empleo de los medios de identificación electrónica anteriormente presentada, y que ya se encontraba, en cierto modo, prevista en el artículo 13.4.b) de la LFE. Este artículo permitía sustituir la presencia personal «[c]uando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años».

Verificación mediante métodos reconocidos a escala nacional

Finalmente, la cuarta posibilidad se encuentra recogida en el numeral d) del artículo 24.1. Es la posibilidad más innovadora legalmente, aunque no desde la perspectiva de las normas técnicas.

Conforme al artículo 24.1 numeral d), la verificación se podrá realizar «utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física». Esta seguridad equivalente deberá ser «confirmada por un organismo de evaluación de la conformidad».

Se trata de una cláusula abierta, que permite introducir opciones alternativas, facilitando la adopción de innovaciones tecnológicas o de proceso, con la triple condición de que:

1) sean admitidos en el nivel nacional,

2) que resulten equivalentes en fiabilidad, lo que se determina en atención a su seguridad,

3) que dicha seguridad haya sido objeto de la correspondiente evaluación.

La noción de reconocimiento a escala nacional implica, en algunos casos, la aparición de normativa específica al respecto, aunque no parece ser una exigencia impuesta por el Reglamento eIDAS. Esta previsión en algunos casos contiene una remisión a lo que se determine reglamentariamente, como sucede en Alemania, por ejemplo, y se ha propuesto en España, caso este último que sigue un enfoque exclusivamente reglamentista quizá basado en un exceso de prudencia.

Otros Estados, en cambio, tratan esta cuestión desde la perspectiva del *soft law* público, como uno de los criterios propuestos por el organismo de supervisión en relación con el procedimiento de cualificación. Este enfoque es mucho más flexible, plenamente alineado con el requerimiento previsto en el artículo 24.1.d) del Reglamento eIDAS de evaluación de conformidad en relación con el nivel de seguridad equivalente a la presencia física. Este enfoque impulsa la adopción rápida de innovaciones, algo beneficioso para la competitividad de los prestadores establecidos en dichos Estados, como por ejemplo en el caso de Austria, de Francia o de Italia.

Entre dichas innovaciones destaca, con gran fuerza, el uso de la identificación a través de la videoconferencia con la persona física, opción ya autorizada en Italia o Francia; o la posibilidad de reutilizar la identificación ya realizada por entidades sujetas a los procedimientos de verificación de la identidad previstos en la normativa de prevención del blanqueo de capitales, como en Italia o Austria.

Cabe, finalmente, preguntarse si resulta posible establecer, en sede nacional, exenciones a la personación que sean diferentes a los cuatro casos anteriores, como por ejemplo sucede en Derecho español con la previsión, ya contenida en el artículo 13.1 de la LFE. En virtud de este artículo «podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado

reconocido ha sido legitimada en presencia notarial». Además, en este caso no se exige formalmente la evaluación de la conformidad a efectos de la determinación de la equivalencia de seguridad.

Parece que esta posibilidad debería rechazarse en una interpretación rigurosa del Reglamento eIDAS, dado que nos encontramos ante un aspecto armonizado, y que además puede afectar negativamente al reconocimiento transfronterizo de los certificados, La razón es que otros Estados miembros consideran, eventualmente, que dichos métodos alternativos no se pueden tratar como equivalentes a la personación. Este problema se puede solventar, en cualquier caso, mediante la reconducción del método en cuestión a la previsión del artículo 24.1.d) ya analizada, que esencialmente sólo implica sujetar todos los métodos alternativos a la evaluación de la conformidad.

2.2.3. La gestión del ciclo de vida del certificado cualificado

El Reglamento eIDAS establece diversas obligaciones relativas a la gestión del ciclo de vida del certificado cualificado. Estas obligaciones pueden ser objeto de complemento o ampliación por parte del legislador nacional, y ademas se orientan a la finalidad identificativa del certificado cualificado.

Así, el numeral k) del artículo 24.2 del Reglamento eIDAS ordena, en primer lugar, que:

> «en caso de los prestadores cualificados de servicios de confianza que expidan certificados cualificados, establecerán y mantendrán actualizada una base de datos de certificados».

En esta base de datos deberán registrarse todos los eventos relativos al ciclo de vida del certificado, y estará sustentada por el correspondiente sistema fiable.

En particular, el Reglamento eIDAS prevé expresamente el registro en esta base de datos de los siguientes hechos:

- la suspensión y la revocación del certificado, a los efectos de la difusión de la información al público acerca del estado de los certificados

- la publicación que constituye condición de eficacia, frente a terceros, de estos cambios de estado

Suspensión de certificados

Respecto a la suspensión de los certificados, ésta produce una pérdida temporal de validez del certificado. El Reglamento eIDAS no regula la suspensión de certificados con carácter obligatorio, sino que remite a lo que establezca en este sentido la normativa nacional. De esta forma nos encontramos ante un elemento de diversidad que podría influir en el funcionamiento del mercado único digital, en el sentido de que los prestadores obligados a ofrecer esta ges-

tión tendrán un mayor coste operacional que sus competidores. No obstante, también es cierto que un cliente podría percibir la suspensión como una ventaja del servicio, en especial en términos de seguridad.

En todo caso, los artículos 28.5 y 38.5 del Reglamento eIDAS, referidos a los certificados de firma electrónica y sello electrónico, respectivamente, prevén dos reglas armonizadas. Por tanto, las mismas deberán recibir un tratamiento uniforme en todos los Estados miembros, en especial al efecto de la necesaria «transparencia cuando y donde esta práctica sea posible», en palabras del Considerando (53) del citado Reglamento eIDAS.

La primera regla, contenida en el numeral a) de los citados apartados, indica que «[s]i un certificado cualificado [...] ha sido suspendido temporalmente, ese certificado perderá su validez durante el período de suspensión», determinando el efecto jurídico asociado a la suspensión, y sin perjuicio de otros efectos que se pudieren, en su caso, establecer en la legislación nacional. Por otro lado, conforme a la segunda regla, contenida en el numeral b), «el período de suspensión se indicará claramente en la base de datos de certificados y el estado de suspensión será visible, durante el período de suspensión, a partir del servicio que proporcione la información sobre el estado del certificado», a los efectos de que dicha condición sea conocida por las partes usuarias.

Como acabamos de ver, el Reglamento eIDAS sólo establece normas relativas a la suspensión de certificados de firma o sello electrónico, pero no de certificados de autenticación de sitio web. Esta laguna genera la duda acerca de si este aspecto puede también ser objeto de regulación por los Estados miembros o, por el contrario, si debe entenderse que no ha de ser legalmente posible suspender certificados cualificados de autenticación de sitio web. Se trata de una laguna que puede resolverse acudiendo a las normas técnicas, en especial si las mismas son adoptadas por la Comisión. Estas normas prohíben, en efecto, la suspensión de certificados de autenticación de sitio web.

Revocación de certificado

Por lo que se refiere a la revocación del certificado, conforme a los artículos 28.4 y 38.4 de Reglamento eIDAS, referidos a los certificados de firma electrónica y sello electrónico, respectivamente, «[s]i un certificado cualificado [...] ha sido revocado después de su activación inicial, perderá su validez desde el momento de su revocación y no podrá en ninguna circunstancia recuperar su estado». Esto no significa que el mismo ya no pueda ser empleado para comprobar la identidad de la persona indicada en el mismo, sino que este uso queda limitado a las pruebas electrónicas respaldadas por dicho certificado que hayan sido creadas con anterioridad a la revocación. Ello es así porque las mismas pruebas pueden ser perfectamente válidas, en función de la causa que ha conducido a la revocación.

En efecto, si la revocación se ha producido como consecuencia de la libre voluntad del titular del certificado, sin que se haya puesto en riesgo la seguridad de la clave privada correspondiente a la clave pública contenida en el certificado, no tiene mucho sentido dejar de confiar en la identidad de esta persona que consta en las pruebas electrónicas que se hayan creado hasta el momento de la revocación. Para ello será preciso que la parte usuaria del certificado pueda determinar la causa de la revocación y su momento temporal preciso. De forma análoga sucede con la suspensión a que nos acabamos de referir.

A ello responden las reglas establecidas en los apartados 3 y 4 del artículo 24 del Reglamento eIDAS. El apartado 3 del artículo 24 ordena que «[c]uando los prestadores cualificados de servicios de confianza que expidan certificados cualificados decidan revocar un certificado, registrarán su revocación en su base de datos de certificados y publicarán el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud», indicando además que «[l]a revocación será efectiva inmediatamente después de su publicación».

Cualesquiera otros elementos relativos a la suspensión o la revocación quedan a lo que establezca el legislador nacional.

> Ejemplo es el establecimiento de causas legales de suspensión o revocación, algo que resulta conveniente en orden a establecer un correcto funcionamiento del mercado. De este modo se expulsan del mismo los certificados potencialmente defectuosos, al tiempo que se protege a los prestadores que expiden los certificados frente a posibles reclamaciones de sus clientes asociadas a la toma de la decisión de suspensión o, en especial, de revocación.

Además, en la autorregulación se encuentran algunas causas, que deben ser adoptadas por los prestadores que se sujetan a la misma. En concreto, la norma ETSI EN 391 411-1 prevé la obligación de proceder a la revocación en los siguientes casos:

- cuando el certificado ya no sea compatible con la política de certificación conforme a la que fue expedido,
- cuando el prestador de servicios sea consciente de cambios que afecten a la validez del certificado,
- cuando la criptografía empleada en el certificado deje de poder garantizar la vinculación entre el titular y la clave pública.

Asimismo, encontramos un completo elenco de causas de revocación en la especificación técnica del CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. Esta especificación resulta aplicable, como ya sabemos, a los certificados cualificados de autenticación de sitio web. Estas quince causas de revocación resultan obligatorias para los prestadores que expiden este tipo de certificado.

No podemos acabar este análisis sin mencionar que, a pesar de lo que se acaba de exponer, el Reglamento eIDAS no establece las consecuencias concretas que implicará la pérdida de validez, temporal o definitiva, del certificado, sobre las firmas o sellos electrónicos creados empleando un certificado inválido. Por ello se deberá estar atento a la normativa aplicable al correspondiente acto jurídico a estos efectos.

Publicación del cambio de estado

El Reglamento eIDAS armoniza una parte de la práctica profesional de los prestadores que expiden certificados. Esta práctica se refiere a dos aspectos:

1) la obligación de registro y publicidad de la revocación, uno de los aspectos de mayor relevancia

2) el plazo correspondiente, que deberá ser el oportuno, y con un máximo de 24 horas en caso de que la misma responda a la solicitud de la persona titular

Nótese que la eficacia de la revocación se produce desde el momento de la publicidad, y no anteriormente, regla que claramente persigue afectar a la responsabilidad del prestador frente a las partes usuarias que hayan confiado en un certificado ya revocado, pero del que no se ha publicado la revocación.

En relación con la publicación de la revocación de la validez del certificado, disponemos del apartado 4 del artículo 24, que complementa al apartado 3 del mismo artículo, pero también los artículos 28.5.b) y 38.5.b) del Reglamento eIDAS.

El apartado 4 del artículo 24 del Reglamento eIDAS ordena que:

> «[l]os prestadores cualificados de servicios de confianza que expidan certificados cualificados proporcionarán a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos».

Este artículo también indica que esta información:

> «deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente».

Esta previsión supone una importante novedad con respecto a la LFE, cuyo artículo 10.4 exigía el mantenimiento de esta información sólo hasta la expiración del certificado. Además, este artículo persigue facilitar la validación de las fuentes de prueba electrónica que se sustentan en dichos certificados, como las firmas electrónicas avanzadas o cualificadas.

Nos encontramos, en este caso, ante normas que persiguen reforzar la función típica del certificado, que resultaría afectada negativamente si no resultara posible a la parte usuaria conocer el estado de validez del certificado, o

si dicho acceso resultase muy gravoso. Estas normas resultan claramente novedosas con respecto a la DFE. Entre estas obligaciones destacan, en primer lugar, la imposición de que el mecanismo de información de estado funcione de forma automatizada y, en segundo lugar, que dicha actuación sea gratuita. Esta previsión legal afecta contundentemente a modelos de negocio como el de la FNMT-RCM, que ha venido cobrando por este servicio, tanto a entidades públicas cuanto a privadas.

2.3. Los efectos jurídicos del certificado electrónico

El Reglamento eIDAS no establece ningún efecto jurídico específico en relación con el uso del certificado electrónico, ni siquiera cuando el mismo es cualificado. Esto es así, seguramente por su carácter accesorio a los procesos a los que sirve de apoyo, y sin perjuicio de que, como hemos visto, de la propia definición del certificado se desprenda claramente que el certificado confirma la identidad de una persona, sea una persona física (un firmante), una persona jurídica (un creador de sellos), o una persona (física o jurídica) titular de un sitio web concreto.

Lo que no existe en el Reglamento eIDAS es, por tanto, una regla de equivalencia funcional con ninguna institución empleada para la prueba de la identidad en las relaciones presenciales o a distancia soportadas en papel.

Más en concreto, el Reglamento eIDAS no autoriza la sustitución de un mecanismo de identidad personal –como podría ser un documento nacional de identidad, en soporte físico– por un certificado electrónico, ni siquiera en el caso de la firma electrónica. Por tanto, el Derecho nacional se ve inalterado al respecto, siempre salvo la posibilidad de que una norma de la Unión establezca esta regla en algún caso concreto.

Por ello, será la normativa de la Unión o la normativa nacional o, cuando resulte posible, la autonomía de la voluntad de las partes, la que permita habilitar, en su caso, esta posibilidad. Y, en su consecuencia, no podrá necesariamente asumirse, con carácter general, que «donde una ley ordene el uso de un documento de identidad, podrá emplearse un certificado de persona física o jurídica», que sería la plasmación a este caso de la regla del equivalente funcional. Esta suerte de regla de equivalencia funcional, que ya hemos visto no existe en el Reglamento eIDAS, no tiene, además, sentido alguno en el caso del certificado de autenticación de sitio web.

Ciertamente, en el Reglamento eIDAS tampoco se establece presunción procesal alguna que apoye el uso de un certificado cualificado, algo que también podrá suceder, sin embargo, en la normativa nacional, si así lo considera necesario el legislador.

3. El servicio de confianza de creación de la firma y sello electrónicos; la posibilidad de delegar la firma o el sello a un tercero

En este apartado estudiamos las características del servicio de confianza de creación de la firma y sello electrónicos, con la posibilidad de delegarlos a un tercero. En primer lugar trabajamos la caracterización del servicio de confianza; en segundo lugar, vemos los requisitos que rigen el servicio, y por último, analizamos los efectos jurídicos asociados a los servicios de confianza.

3.1. Caracterización del servicio

Estudiamos el servicio de confianza de la creación de firmas y sellos teniendo en cuenta la posibilidad de hacerlo a distancia, y la autorización a un tercero a utilizar los datos de creación de firma o sello.

3.1.1. Creación de firmas y sellos a distancia

Una de las grandes novedades del Reglamento eIDAS consiste en el servicio de creación de firma o sello por parte de un prestador de servicios, que habilita las operaciones relativas a la creación de la firma electrónica, mediante el dispositivo correspondiente. Esta opción se ha venido denominando «firma delegada», o «firma centralizada», o «firma remota», o incluso «firma en la Nube». Hasta la aparición del Reglamento eIDAS había generado dudas acerca de su legalidad.

Sin embargo, como expone el Considerando 51 del Reglamento eIDAS:

> «debe ser posible para el firmante confiar a un tercero los dispositivos de creación de firmas electrónicas cualificados».

Esta posibilidad viene referida a diversos casos de uso, incluyendo la cesión de un dispositivo como una tarjeta criptográfica (típicamente para su uso desatendido), o, de forma más prometedora, al empleo de sistemas de clave privada centralizada (HSM) a que nos hemos referido anteriormente.

Asimismo, el Considerando 52 del Reglamento eIDAS aclara que:

> «debido a sus múltiples ventajas económicas, debe desarrollarse la creación de firmas electrónicas a distancia con un entorno de creación de firma electrónica gestionado por un proveedor de servicios de confianza en nombre del firmante».

Esta posibilidad es conceptualmente diferente a la anterior, y más amplia, al referirse no sólo a la gestión del dispositivo cualificado, sino a la creación de la firma, sea la misma avanzada o cualificada.

Estas normas suponen un claro avance respecto a la normativa anterior, que no parecía admitir la posesión de los datos de creación de firma por ninguna persona diferente del firmante. Además, el despliegue de los dispositivos seguros de creación de firma electrónica ha planteado dificultades técnicas; aunque hasta ahora han sido comúnmente aceptados en especial en entornos de movilidad. Estos dispositivos son tarjetas con microprocesador criptográfico. Por ello, es posible que esta opción de creación de firmas por un proveedor de servicios facilite de forma muy importante la adopción de la firma o sello electrónico cualificado.

En su consecuencia, el Reglamento eIDAS permite la existencia del servicio de creación de firma o sello electrónico a distancia, pudiendo ser ordinaria, avanzada, avanzada basada en certificado no cualificado o avanzada basada en certificado cualificado. No obstante, no considera el servicio cualificado de creación de firma electrónica cualificada o de sello electrónico cualificado como un servicio independiente, sino que el mismo deberá ser parte de un servicio cualificado tipificado en el propio Reglamento eIDAS que ofrezca un prestador cualificado.

O, por ser más preciso, y como veremos inmediatamente, lo que el Reglamento eIDAS permite es el servicio (siempre sin cualificación) de creación de firma o sello electrónico a distancia. Esta firma o sello podrá ser cualificado incluso aunque un tercero genere o gestione en su nombre los datos de creación correspondientes. Para ello empleará un dispositivo remoto bajo la responsabilidad del prestador cualificado. Desde esta concepción, lo que el Reglamento eIDAS no permitiría es la existencia de un hipotético servicio cualificado de generación y gestión de claves por cuenta del firmante o del creador de sellos.

Sistema Cl@ve firma

Este enfoque técnico de firma con clave centralizada es el que sustenta el sistema Cl@ve firma, que permite la obtención de un certificado de firma del DNI electrónico sin necesidad de disponer de la correspondiente tarjeta soporte. Este sistema ya se emplea en diversos servicios de administración electrónica, y otros servicios análogos ofrecidos ya por diversos prestadores o autoridades en la Unión Europea.

La finalidad típica del servicio será, normalmente, permitir al firmante o creador de sellos proceder a la generación de la firma electrónica o del sello electrónico de forma remota, sin tener que disponer en su poder físico del correspondiente dispositivo de creación, en especial en el caso de un dispositivo cualificado.

3.1.2. Autorización a un tercero a utilizar datos de creación de firma o sello

Este servicio de creación de firma o sello a distancia, antes mencionado, implica que el prestador disponga de los correspondientes componentes técnicos para la generación y/o gestión de los datos de creación de firma o sello por

cuenta del usuario. Diferente al servicio de creación de firma o sello a distancia es la posibilidad de que un firmante o creador de sello autorice a un tercero a utilizar los datos de creación de firma o sello. Esto puede anticiparse bastante polémico.

No nos encontramos en este caso ante un prestador de servicios de confianza que genera o gestiona datos de creación de firma o sello que se mantienen bajo el control exclusivo, con un alto nivel de confianza, del firmante o creador de sellos, sino que nos encontramos ante un negocio jurídico diferenciado, en cuya virtud se encomienda a un tercero la utilización de los datos de creación de firma o sello en cuestión. Se trata de un tercero que actuará por cuenta del firmante o del creador del sello.

Tal negocio jurídico, sustentado en la autonomía de la voluntad de las partes, será lícito en tanto en cuanto cumpla con los requisitos generales contenidos en la legislación, significativamente, el Código Civil español (en adelante, CC). En este sentido, conforme a lo establecido en el artículo 1255 del CC, «los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral ni al orden público», por lo que se deberá determinar previamente la existencia de alguna prohibición legal al respecto.

La posibilidad de que el firmante o creador de sellos pueda autorizar a un tercero la utilización de los datos de creación no se encuentra expresamente regulada en el Reglamento eIDAS, y tampoco se encontraba regulada en la normativa anterior (ni en la LFE, ni en la DFE). Por ello, no puede hablarse de una autorización expresa al respecta, ni de que su ejercicio se encuentra autorizado, pero con sujeción a condiciones específicas, como sucede en el caso de la generación y gestión de los datos de creación de firma y sello a la que antes nos hemos referido.

Pero esta posibilidad tampoco se encuentra claramente prohibida en la normativa, ni siquiera indirectamente, sino que el Reglamento eIDAS emplea una terminología que claramente ubica esta cuestión en el ámbito del riesgo del firmante o creador de sello.

Recuérdese, a tal efecto, que el artículo 26.c) del Reglamento eIDAS se refiere a que la firma electrónica avanzada debe:

> «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».

Obsérvese que dice que el firmante «puede utilizar», cuando podría haber dicho que los datos «debían ser utilizados» bajo su control exclusivo. En el mismo sentido, observamos en el artículo 36.c) del Reglamento eIDAS, que dispone como uno de los requisitos para los sellos electrónicos avanzados:

> «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».

Otro ejemplo es el Anexo II, epígrafe 1.d) del mismo Reglamento, cuando determina que el dispositivo cualificado garantizará –aplicable *mutatis mutandis* a los sellos electrónicos– que:

> «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».

De nuevo observamos que dice que «pueden ser protegidos», cuando podría haber dicho que dichos dispositivos debían impedir el uso de los datos de creación por parte de terceros.

Tampoco la LFE estableció un deber legal de uso personal e intransferible de los datos de creación de firma electrónica (de persona física o de persona jurídica). Más bien situó la cuestión en el ámbito de la responsabilidad y, para ser más exactos, en el sentido de establecer una limitación de responsabilidad del prestador que expidió el certificado en caso de «negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de éstos o, en su caso, de los medios que den acceso a ellos»[6]. En este caso el responsable será, lógicamente, el firmante (o, por analogía, el creador de sellos).

(6)Artículo 23.1.c) de la LFE.

El legislador de la Unión podría haber configurado la utilización de los datos de creación de firma –no los de sello, por su propia naturaleza– como una actuación estrictamente personal, imponiendo la correspondiente obligación *ex lege*. No obstante, no lo ha hecho, por lo que cabe concluir que sería conforme a Derecho que un firmante o creador de sello autorizase a un tercero a la utilización de sus datos de creación, a salvo de lo que pueda disponer el legislador nacional.

En este sentido, la principal limitación que cabe imaginar a esta posibilidad reside en la hipotética prohibición que, al respecto, pueda establecer el prestador de servicios de confianza que expide al certificado, dado que en ese caso nos encontraremos ante un incumplimiento de una obligación del contrato de certificación, posiblemente considerada esencial por el prestador, y que conducirá, cuanto menos, a la revocación del certificado y, como ya se ha adelantado, a la exoneración de la responsabilidad por parte del prestador del servicio de confianza que expidió el certificado.

En este sentido, cabe recordar que el artículo 18.b) de la LFE –que ha sido desplazado parcialmente por el Reglamento eIDAS– obliga en su numeral primero a informar al firmante de la forma en que deben custodiarse los datos

de creación de firma, por lo que normalmente nos encontraremos ante una obligación contractual, estrictamente personal e intransferible, de utilización de los datos de creación de firma.

Por tanto, para que se pueda implementar sin riesgo esta posibilidad de autorización de utilización de datos de creación de firma o sello a un tercero será importante que el prestador no establezca este tipo de prohibición.

Adicionalmente, será absolutamente imprescindible que el firmante o creador de sello legítimo pueda, en cualquier momento, conceder y retirar dicha autorización. Además, será imprescindible que la autorización se encuentre limitada exactamente a una persona, a los efectos de disponer de la necesaria trazabilidad en la utilización de los datos de creación de firma o sello correspondientes.

Por último, es necesario indicar que esta autorización de la utilización de los datos de creación de firma o sello por parte de un tercero puede realizarse en cualquiera de las dos situaciones:

- Cuando el firmante o creador de sellos posee físicamente del dispositivo –en su caso, cualificado– de creación de firma o sello (por ejemplo, entregando su tarjeta criptográfica al tercero).

- Cuando la gestión de los datos de creación de firma o sello se ha encomendado a un prestador de servicios de confianza, como acabamos de ver.

A pesar de dar autorización, lo que no se deberá hacer es proceder a la copia de los datos de creación de firma o sello electrónico y su entrega a un tercero que no tenga esta condición de prestador de servicios de confianza. Efectuar una copia resulta excesivamente arriesgado para el firmante o creador de sello.

Esta práctica sería, además, considerada ilegal en el caso de la firma o sello electrónica/o cualificada/o, por contravenir los requisitos del servicio a los que nos referimos a continuación.

3.2. Los requisitos del servicio

Los requisitos del servicio de confianza de creación de firma y sello contemplan la garantía del control exclusivo de los datos. Por ello, vamos a estudiar tres aspectos. En primer lugar, el establecimiento de procedimientos y mecanismos de control, y seguridad de la gestión y administrativos, y canales de comunicación electrónica seguros. En segundo lugar, vemos los requisitos aplicables a los proveedores de servicios de confianza. Por último, analizamos la posibilidad de duplicar datos de creación en aras a tener copias de seguridad, pero preservando siempre la seguridad de los datos.

3.2.1. Procedimientos y mecanismos de control exclusivo de datos de creación

Como punto de partida, debemos considerar que el firmante debe tener el control exclusivo de los datos. A este fin, para confiar a un tercero los dispositivos de creación de firmas, el firmante debe saber que este tercero aplica **procedimientos y mecanismos adecuados que garanticen el control** exclusivo de los datos. En este sentido, el Considerando 51 del Reglamento eIDAS condiciona la posibilidad de que un firmante confíe a un tercero los dispositivos de creación de firmas electrónicas cualificados, está condicionada a:

> «que se apliquen los procedimientos y mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de la firma electrónica y que la utilización del dispositivo cumple los requisitos de la firma cualificada».

Asimismo, en el caso de las firmas creadas por un tercero, para garantizar el reconocimiento jurídico también se deben tener definidos **procedimientos de seguridad de la gestión y administrativos, sistemas y productos fiables y canales de comunicación electrónica seguros.** Así, el Considerando 52 del Reglamento eIDAS aclara que:

> «a fin de garantizar que estas firmas electrónicas obtengan el mismo reconocimiento jurídico que las firmas electrónicas creadas en un entorno completamente gestionado por el usuario, los proveedores que ofrezcan servicios de firma a distancia deben aplicar procedimientos de seguridad de la gestión y administrativos específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas electrónicas es fiable y se utiliza bajo el control exclusivo del firmante».

En ese caso, no sólo nos referimos a un gestor centralizado de claves, sino a todo el entorno de creación de la firma electrónica a distancia gestionado por un tercero mediante el correspondiente sistema fiable.

3.2.2. Requisitos aplicables a los proveedores

Más relevante resulta la potente limitación a esta posibilidad de que el firmante confíe en un tercero la creación de firmas electrónicas cualificadas. Esta limitación la encontramos en la frase final del Considerando 52 del Reglamento eIDAS, cuando indica que:

> «en el caso de una firma electrónica cualificada creada mediante un dispositivo de creación de firmas electrónicas a distancia, se aplicarán los requisitos aplicables a los proveedores de servicios de confianza cualificados contemplados en el presente Reglamento».

Estos requisitos principalmente se encuentran regulados en los artículos 19 y 24 del Reglamento eIDAS. Esta limitación sabemos que se refiere también a la creación del sello electrónico cualificado a distancia, por la aplicación *mutatis mutandis* al sello mismo de los requisitos de la firma electrónica cualificada.

En concreto, el apartado 3 del Anexo II del Reglamento eIDAS, aplicable tanto a dispositivos de creación de firma cualificados, como a dispositivos de creación de sello cualificados, indica que:

> «la generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante sólo podrán correr a cargo de un prestador cualificado de servicios de confianza».

Como ya dijimos anteriormente, dado que en el Reglamento eIDAS no considera la creación de firma o sello como un servicio que pueda ser objeto de cualificación, dicho prestador deberá encontrarse cualificado para prestar cualquiera de los servicios que sí pueden ser objeto de cualificación.

Esta posibilidad existe también en entornos corporativos, donde los datos de creación de la firma electrónica del empleado son gestionados en dispositivos de firma centralizada bajo la responsabilidad del empleador, por ejemplo, a condición de que se cualifique como prestador.

3.2.3. Duplicar datos de creación de firma

Por su parte, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma podrán duplicar los datos a efectos de realizar copias de seguridad. En concreto el apartado 4 del Anexo II del Reglamento eIDAS, determina que:

> «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:
>
> - la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;
> - el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio».

Se trata de una previsión orientada a garantizar al máximo la seguridad de los datos de creación de firma o sello electrónico, en cuya virtud se restringen las operaciones que el prestador puede realizar sobre dichos datos. Más en concreto, la norma autoriza la duplicación de los datos de creación a los solos efectos de realizar una copia de seguridad de los mismos, pero con tres condiciones.

En primer lugar, el procedimiento de duplicación de los datos de creación de firma o sello electrónico no debe afectar negativamente a la posibilidad de que los citados datos de creación puedan ser protegidos de forma fiable frente a su utilización por terceros. De ello se desprende la necesidad de que el acceso a la versión duplicada de los datos de creación se encuentre bajo el mismo grado de control exclusivo de uso que los datos originales gestionados por el prestador.

En segundo lugar, los conjuntos de datos duplicados no deben ser de un nivel de seguridad inferior a los originales, con el objetivo evidente de impedir la sustracción de dichos datos, con la consiguiente posibilidad de suplantar la identidad del firmante o del creador de sellos, actuando en su lugar sin detección. Se trata de un requisito que se puede cumplir empleando técnicas de cifrado o de partición de claves en fragmentos, antes de su almacenamiento en el exterior del dispositivo cualificado de creación de firma o sello.

En tercer, y último lugar, se restringe la producción de estos conjuntos duplicados de datos de creación de firma o sello electrónico a los que sean estrictamente necesarios para mantener la continuidad del servicio.

Se trata, de nuevo, de una norma limitativa que persigue reducir la exposición a riesgos de los datos de creación de firma o sello electrónico, dado que cuanto menor sea el número de conjuntos de datos duplicados, menor será también la probabilidad de que terceros accedan a estos datos duplicados de forma ilegítima.

El Reglamento eIDAS no establece más requisitos específicos en relación con este servicio, al que resultan también aplicables los requisitos generales aplicables a los prestadores de servicios de confianza, sin cualificación o con ella.

3.3. Los efectos jurídicos asociados al servicio

El Reglamento eIDAS no establece ningún efecto jurídico específico para este servicio, dado que el efecto jurídico se establece, como hemos visto, en relación con la prueba electrónica (la firma o sello electrónico) que se crea al hacer uso del mismo.

4. El servicio de confianza de validación de la firma y sello electrónicos

Estudiamos el servicio de confianza de validación de la firma y sello electrónicos teniendo en cuenta tres aspectos. En primer lugar, vemos los aspectos que caracterizan el servicio. En segundo lugar, estudiamos los requisitos del servicio. Por último, vemos los efectos jurídicos asociados.

4.1. Caracterización del servicio

En este subapartado estudiamos la caracterización del servicio, a partir de tres aspectos. En primer lugar, analizamos las características específicas del prestador del servicio de confianza de validación de firma y sello electrónicos. En segundo lugar, vemos las características de a quién se ofrece el servicio. Por último, identificamos las características de la reutilización de un servicio cualificado de firma o sello electrónico cualificado para la validación de una firma o sello electrónico.

4.1.1. Características del prestador del servicio

Como en otros casos, se puede ofrecer un servicio cualificado, que cumplirá los requisitos que establece el Reglamento, o un servicio sin cualificación, en cuyo caso realmente los requisitos serán establecidos por el propio prestador.

> El servicio de validación permite la comprobación de una firma o sello electrónico, de forma que se determine su validez y, por tanto, su capacidad para producir los efectos jurídicos deseados.

Respecto a este servicio de confianza, en su modalidad cualificada, la especificación de los requisitos exigibles a los prestadores de un servicio de validación contamos con el Considerando (57) del Reglamento eIDAS. Este considerando indica que «la especificación de los requisitos exigibles a los prestadores cualificados de servicios de confianza que pueden brindar un servicio de validación cualificado a las partes usuarias que no desean o no pueden realizar por sí mismas la validación de las firmas electrónicas cualificadas debe estimular a los sectores privado y público para que inviertan en tales servicios», con el objeto de facilitar el empleo de la firma o sello electrónico.

Se trata de otra de las novedades del Reglamento eIDAS en relación con la DFE, que no regulaba servicio alguno al respecto. La DFE se limitaba, en su Anexo III, a establecer una serie de recomendaciones para la verificación segura de la firma electrónica. Estas recomendaciones en la LFE se convirtieron en obligación, referida a los dispositivos de verificación de firma electrónica.

A pesar de resultar novedoso en el Reglamento eIDAS, se trata de un servicio que ha venido siendo ampliamente empleado en España, en especial en el ámbito de la Administración electrónica, y que se encuentra parcialmente regulado en el Real Decreto del Esquema Nacional de Interoperabilidad (RDENI). Resultan muy relevantes al menos en volumen, las siguientes tres experiencias:

1) el servicio @firma, la solución tecnológica en la que se basa la Plataforma de validación y firma electrónica de la administración española, puesta a disposición de otras administraciones públicas,

2) el servicio Validador del Consorci Administración Oberta de Catalunya,

3) la plataforma Zain del Izenpe vasco.

La novedad del Reglamento es, en definitiva, la **tipificación**, la **armonización** y el **fomento del servicio de validación**. Esto es así seguramente por dos razones. En primer lugar por la enorme complejidad técnica asociada a esta tarea, que hace francamente difícil, a los terceros que reciben firmas o sellos electrónicos, algo aparentemente tan simple como asegurarse de que son válidos. En segundo lugar, la regulación de la validación es para crear un marco que permita consensuar las reglas para proceder a dicha validación de forma consistente en toda la Unión Europea.

Este último aspecto no es precisamente baladí, en especial en el caso de las firmas electrónicas transfronterizas, porque la ley aplicable a la creación y a la validación de la firma electrónica son diferentes, algo que en el modelo de la DFE ha generado problemas de reconocimiento transfronterizo de las firmas electrónicas. Esta disfunción debería resolverse mediante el enfoque de armonización del Reglamento eIDAS, al menos en el caso de la firma y el sello electrónico cualificado, dado que ahora la norma aplicable es únicamente el propio Reglamento eIDAS, que es igual para toda la Unión.

Al estudiar la validación debemos tener en cuenta tanto el **proceso** de verificar y confirmar como los **datos utilizados para validar**. La validación se define en el artículo 3.41) del Reglamento eIDAS como «el proceso de verificar y confirmar la validez de una firma o sello electrónicos», mientras que los datos de validación se definen, en el artículo 3.40) del propio Reglamento, como «los datos utilizados para validar una firma electrónica o un sello electrónico».

4.1.2. A quién se ofrece

Resulta interesante notar que este **servicio se ofrece**, normalmente, **a una persona** que recibe una firma o sello electrónico calificado, y precisa realizar este proceso de forma previa a confiar en dicha firma o sello electrónico cualificado. Esta parte usuaria se define, en el artículo 3.6) del Reglamento eIDAS, como «la persona física o jurídica que confía en [...] el servicio de confianza», aunque realmente, como hemos avanzado, realmente precisa confiar en la prueba electrónica recibida[7]. Obviamente, el servicio también se puede prestar al firmante o al creador de sellos, para que posteriormente remita la firma o sello electrónico cualificado a terceros, o para conservarla junto con el documento o mensaje.

(7)Como una prueba de identificación electrónica, una firma o sello electrónico, o un sello de tiempo electrónico, o una certificación de entrega electrónica.

4.1.3. Reutilización de un servicio cualificado

Nótese que, como en otros casos, se puede ofrecer un servicio cualificado, que cumplirá los requisitos que establece el Reglamento, o un servicio sin cualificación, en cuyo caso realmente los requisitos serán establecidos por el propio prestador.

En este sentido, hay que dejar claro que el proceso, y el correspondiente servicio cualificado, se refiere a la validación de la firma o sello electrónico cualificado, y no a la validación de otras tipologías de firma o sello electrónico, algo que responde a la imposibilidad de establecer requisitos para todas las posibles tecnologías que sustentan la prueba de atribución. Ello no significa que no se pueda «reutilizar» un servicio cualificado de firma o sello electrónico cualificado para la validación de una firma o sello electrónico avanzado basado en un certificado cualificado. Esto es algo relativamente simple dado que únicamente debe obviarse la comprobación de uno de los requisitos de la firma o sello, que además se informa en el certificado cualificado. Más difícil resulta reutilizar este proceso cuando nos encontramos ante un certificado sin cualificación, por no encontrarse normalizada la información correspondiente al mismo, y así sucesivamente.

4.1.4. Requisitos del proceso de validación

El enfoque del Reglamento eIDAS es muy pragmático y centra la cualificación en el proceso de validación de firma o sello electrónico cualificado, el más concreto y mejor definido en la normativa, tanto jurídica, como técnica. A continuación, analizaremos sucintamente estos requisitos, los cuales mostrarán la complejidad que subyace a este proceso, que –recuérdese– debe ser automático, y que consta de diversos elementos en juego.

Validación de certificados cualificados de firma o sello electrónico cualificado

En primer lugar, el artículo 32.1 del Reglamento eIDAS contiene algunas normas referidas a los certificados cualificados de firma o sello electrónico cualificado. En concreto, en el proceso de validación se debe verificar que el certificado que respalda la firma o sello electrónico cualificado era, en el momento de la creación de la firma, un certificado cualificado de firma electrónica ajustado al anexo I o al anexo III del Reglamento eIDAS, respectivamente. Se trata de un requisito que exige, como se puede fácilmente deducir, cumplir dos requisitos:

1) Acceder al contenido del certificado y evaluar la completitud y corrección de dichas informaciones, o alternativamente, obtener información adicional acerca de los certificados. Esta información se puede extraer posiblemente de la lista de confianza publicada por el órgano competente.

2) Poder determinar que esta información era correcta en el momento de creación de la firma, para lo cual es imprescindible determinar con certeza este aspecto, siendo muy relevante el uso de un servicio, eventualmente cualificado, de sellado de tiempo electrónico en un momento muy cercano al de creación de la firma o sello electrónico cualificado.

También debe ser objeto de comprobación que el certificado cualificado en cuestión había sido emitido por un prestador de servicios de confianza. Esto requiere de la comprobación de la información contenida en la lista de confianza anteriormente mencionada, y acceder a la fecha de creación de la firma o sello electrónico cualificado, y que era válido en el momento de la firma. Para ello se requiere acceder a la información de estado de dicho certificado, de nuevo a la fecha de creación de la firma o sello electrónico. En consecuencia, también se debe comprobar el certificado empleado por el prestador para firmar el certificado del firmante o creador de sello, así como, en su caso, el certificado que a su vez hubiera firmado el certificado del prestador, y así hasta el inicio de la jerarquía.

Informaciones que deben mostrarse

En segundo lugar, el mismo artículo 32.1 contiene algunas exigencias relativas a algunas informaciones que deben mostrarse, de forma garantizada, a la parte usuaria. Estas informaciones deben incluir los datos de validación de firma o sello, el conjunto único de datos que representa al firmante o creador de sellos en el certificado o una indicación clara acerca de haberse utilizado un seudónimo, en lugar de la identidad real del firmante.

Se trata de requisitos orientados a sustentar las garantías de la firma o sello electrónico asociadas a los datos contenidos en el correspondiente certificado. De este modo la parte usuaria puede conocer la identidad –en su caso, basada en seudónimo– del firmante o creador de sellos, y los datos de validación de

la firma o sello. Esto es, el usuario conoce la clave pública correspondiente a la persona identificada en el certificado en cuestión, dado que estos datos permiten determinar que una firma o sello es efectivamente avanzado.

Comprobaciones de la firma o sello electrónicos

En tercer lugar, el artículo 32.1 del Reglamento eIDAS se refiere a exigencias específicas de la firma o sello electrónico, entre las cuales se encuentran las comprobaciones de los siguientes aspectos:

- Que la firma o sello han sido creados empleando un dispositivo cualificado. Ello se puede hacer mediante la información contenida en el certificado correspondiente, o alternativamente mediante la información indicada en la lista de confianza.

- Que se ha mantenido la integridad de los datos firmados o sellados, y finalmente, de que en el momento de firma se han cumplido todos los requisitos previstos para considerar a la firma o sello como avanzados.

Esto último implica que el proceso de validación ha de ser capaz de comprobar los siguientes aspectos:

- La vinculación entre firma o sello y firmante o creador de sello, respectivamente.

- Que la firma o sello identifica a firmante o creador de sello. Ello resulta redundante con la comprobación ya realizada del certificado.

- El control exclusivo de los datos de creación de firma o sello, que sólo puede asumirse como correcto a partir de la constatación del uso del dispositivo cualificado, que ya sabemos que es puramente declarativa.

- La vinculación entre firma o sello y datos firmados o sellados.

Se trata de una redacción ciertamente oscura, que desde luego no facilita la comprensión del proceso –por no mencionar la enorme complejidad y coste que puede suponer una prueba pericial en estas condiciones. Este problema, como ya hemos visto en otros casos, sólo se mitiga gracias a la existencia de especificaciones y normas técnicas que concretan los diferentes requisitos, al objeto de que las diversas aplicaciones sean realmente capaces de validar la firma o el sello cualificado.

4.1.5. Especificaciones y normas técnicas

Al amparo de las recomendaciones contenidas en la DFE, se aprobó la especificación técnica CEN CWA 14171:2004, sobre procedimientos de verificación de firma electrónica, que ha sido recientemente actualizada en el TC 224 de CEN, para su conversión en la norma europea EN 419 111, partes 1, 4 y 5.

Más relevante, incluso, es la importante norma ETSI EN 319 102-1, que define de forma completa y minuciosa el proceso de validación de firma o sello electrónico, dada la posibilidad, que ya conocemos, de que la misma sea establecida a efectos de la acreditación de la conformidad del proceso. En efecto, el artículo 32.3 del Reglamento eIDAS prevé que:

> «[l]a Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a la validación de las firmas electrónicas cualificadas».

De este modo «se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la validación de una firma electrónica cualificada se ajuste a dichas normas». Estos actos de ejecución deben adoptarse «con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2». Es de resaltar que hasta hoy ninguna norma se ha establecido.

En concreto, esta norma prevé tres modalidades del proceso de validación de firma o sello electrónico en función de las necesidades de la parte usuaria.

La primera modalidad del proceso prevista es la **validación de una firma o sello electrónico básico**, que devuelve como resultado el estado de validez de la firma o sello en el momento de la validación. Esta clase de firma o sello se puede validar mientras el certificado no haya sido revocado ni haya expirado en el momento de la validación. Por ello, esta modalidad no es suficiente para las firmas o sellos sujetos a obligaciones legales de conservación a largo plazo.

La segunda modalidad del proceso prevista es la **validación de una firma o sello con tiempo y disponibilidad a largo plazo de materiales de validación**, que devuelve como como resultado el estado de validez de la firma o sello en el momento temporal más antiguo en el que se puede demostrar su existencia. Por ello, esta modalidad se puede emplear para comprobar la validez de una firma o sello incluso después de la revocación del correspondiente certificado. Además, cuando se incorporan estos materiales de validación, como las listas de revocación de certificados, este proceso dispone de ellos a largo plazo para efectuar dichas validaciones. Es preciso, con todo, hacer notar que esta firma o sello se podrá validar sólo mientras estos materiales de validación estén vigentes.

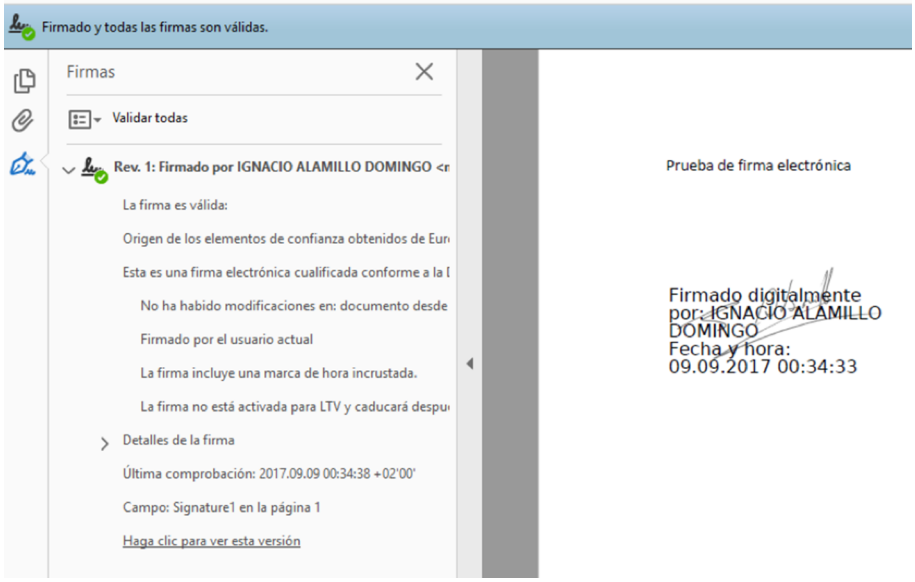
4.1.6. Resultado del proceso de validación

Finalmente, el epígrafe 2 del artículo 32 del Reglamento concreta que:

> «[e]l sistema utilizado para validar la firma electrónica cualificada ofrecerá a la parte usuaria el resultado correcto del proceso de validación y le permitirá detectar cualquier problema que afecte a la seguridad».

Esta previsión se centra en el producto –típicamente una aplicación informática– que implanta el proceso de validación, como se puede ver en la siguiente ilustración.

Figura 1



En este sentido, es preciso aclarar que el proceso de validación de la firma o sello electrónico puede devolver tres resultados principales. Estos resultados son:

1) *Total-passed*. Este resultado se produce cuando se han validado correctamente todos los elementos de la firma o sello electrónico.

2) *Total-failed*. Este resultado se produce cuando se dan alguno de los siguientes casos:

a) ha fallado la comprobación criptográfica de la firma o sello,

b) se ha comprobado que la firma o sello fue creado después de la revocación o expiración del certificado,

c) que la firma o sello es sintácticamente incorrecto.

3) *Indeterminate*. Este resultado se produce cuando alguna comprobación ha fallado, pero de ello no se desprende que la firma o sello sea necesariamente inválido, como por ejemplo cuando se valida una firma respaldada por un certificado expirado, porque en realidad dicha firma podría ser válida, siempre que se pueda determinar que fue creada antes de la expiración del certificado. Esto se podría acreditar si el documento y la firma han sido, por ejemplo, conservados en un archivo con las suficientes garantías.

4.2. Los requisitos del servicio

Como hemos visto, el Reglamento eIDAS define los elementos esenciales del proceso de validación de una firma o sello electrónico cualificado en los artículos 32.1 y 40, respectivamente, por lo que el servicio cualificado ofrecido deberá garantizar su cumplimiento.

En efecto, conforme al artículo 33.1.a) del Reglamento eIDAS –aplicable también al sello electrónico en virtud de lo establecido en el artículo 40 del propio Reglamento–, «[s]olo podrá prestar un servicio de validación cualificado de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que […] realice la validación de conformidad con el artículo 32, apartado 1 […]», proceso al que nos hemos referido en el apartado inmediatamente anterior.

Adicionalmente, conforme al numeral b) del mismo artículo 33.1 del Reglamento eIDAS, se requiere al prestador del servicio que:

> «permita que las partes usuarias reciban el resultado del proceso de validación de una manera automatizada que sea fiable, eficiente e incluya la firma electrónica avanzada o el sello electrónico avanzado del prestador cualificado de servicio de validación».

El artículo 33.1 se refiere a una suerte de **informe de validación** de la firma o sello electrónico, que va a servir como prueba electrónica justificativa de haberse realizado la citada validación.

Respecto a lo que debería incluir el citado informe, de nuevo resulta relevante la ya mencionada norma ETSI EN 319 102-1. Esta define los contenidos principales del resultado del proceso de validación de firma o sello electrónico, en sus diferentes variantes, puesto que también en este caso existe la posibilidad de que la misma sea establecida a efectos de la acreditación de la conformidad del servicio.

De esta forma, el artículo 33.2 del Reglamento eIDAS prevé que «[l]a Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas al servicio de validación cualificado al que se refiere el apartado 1», de modo que «se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la validación de una firma electrónica cualificada se

ajuste a dichas normas». Estos actos de ejecución deben adoptarse «con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2»; y sin que hasta hoy se haya establecido norma alguna.

El mismo artículo 33.1 del Reglamento eIDAS prevé la posibilidad de que el informe sea de procesamiento automático, sin perjuicio de que la información sea presentada de forma comprensible para las partes usuarias que lo requieran. Algunas de las informaciones que se incluyen son informaciones como:

- una indicación del estado correspondiente a los resultados del proceso de validación
- una indicación de la política de validación o del conjunto de condiciones aplicables a la validación
- la fecha y hora de la firma o sello que fue determinada en la validación y los datos de validación empleados para ello
- la modalidad de proceso de validación empleada
- determinadas informaciones adicionales, en función del resultado.

El Reglamento eIDAS no establece más requisitos específicos en relación con este servicio, al que resultan también aplicables los requisitos generales aplicables a los prestadores de servicios de confianza, sin cualificación o con ella.

4.3. Los efectos jurídicos asociados al servicio

El Reglamento eIDAS no establece ningún efecto jurídico expreso y específico para este servicio. No obstante, es innegable que el resultado del servicio –el informe de validación– es un elemento especialmente orientado a dos aspectos. En primer lugar, el informe de validación está orientado a la facilitación de la prueba (administrativa o judicial) de la firma o sello electrónico cualificada, en especial desde el punto de vista de la parte usuaria. Ésta en muchas ocasiones precisará asistencia para estas tareas. En segundo lugar, el informe de validación facilita la libre circulación de las firmas y sellos electrónicos cualificados dentro de la Unión Europea. Se trata, en sí mismo, de una prueba electrónica relativa a la prueba electrónica que es la firma, en relación con el documento o mensaje firmado.

Sin embargo, este efecto jurídico implícito del servicio se dará, con su máxima intensidad, cuando la Comisión Europea establezca las correspondientes normas técnicas de proceso y servicio, puesto que está fuera de toda duda el valor de disponer de un informe de validación con valor de presunción de conformidad con los requisitos legales correspondientes.

Sin embargo, el hecho de que no se establezca, en el Reglamento eIDAS, un efecto jurídico específico para este servicio de confianza no significa que no se pueda establecer en sede nacional.

5. El servicio de confianza de conservación de la firma y sello electrónico

En este apartado estudiamos la prestación de servicios de confianza de conservación de la firma y sello electrónico, a partir de tres temas. En primer analizamos los aspectos que componen la caracterización del servicio. En segundo lugar, trabajamos los requisitos del servicio. Por último, vemos los efectos jurídicos asociados al servicio.

5.1. Caracterización del servicio

El servicio de conservación de firma o sello electrónico permite ampliar la fiabilidad de los datos de validación de la firma o sello electrónico cualificado más allá de su período de validez tecnológica inicial. Esta necesidad deriva de la tecnología criptográfica empleada, que pierde fortaleza a medida que transcurre el tiempo, principalmente por el incremento de la capacidad de cálculo y por la posible aparición de ataques que puedan afectar negativamente a los algoritmos.

Esta necesidad conecta con la existencia de documentos o mensajes de duración superior al de una firma o sello electrónico, por lo que hay que mantener su validez jurídica. El Reglamento eIDAS identifica con bastante claridad esta necesidad, en su Considerando (61). En él indica que la norma:

> «debe garantizar la conservación a largo plazo de la información, es decir, la validez jurídica de la firma electrónica y los sellos electrónicos durante períodos de tiempo prolongados, garantizando que se puedan validar independientemente de la evolución futura de la tecnología».

Esto es así, porque de otro modo se podrían ver afectadas las garantías de autenticidad e integridad del documento al que se han incorporado dichas firmas electrónicos y sellos electrónicos.

Este objetivo se podrá lograr acudiendo a diversas técnicas. Algunas de estas técnicas son la incorporación, de forma protegida, de informaciones adicionales a la firma o sello electrónico o el empleo de repositorios de documentos firmados. Estas técnicas han sido inicialmente reguladas actualmente en la normativa nacional, que cabe imaginar quedará superada por la regulación europea, aplicable también al sector privado.

La regulación nacional

Un ejemplo de regulación nacional es el caso de España, donde las técnicas se regulan en la normativa de administración electrónica.

Antes de entrar en los requisitos del servicio, conviene hacer notar que el Reglamento eIDAS, a diferencia de la creación y validación de firma y sello electrónico, no regula cómo pueden el firmante o creador de sellos, o la parte usuaria (por ejemplo, el receptor del documento o mensaje firmado o sellado) conservar dicha firma o sello electrónico cualificado. Esto es algo francamente criticable por la evidente incompletitud que supone dicha laguna.

5.2. Los requisitos del servicio

En este subapartado vemos las características de los prestadores del servicio y las especificaciones del servicio.

5.2.1. Características de los prestadores del servicio

En este marco, el artículo 34.1 del Reglamento eIDAS –aplicable también al sello electrónico en virtud de lo establecido en el artículo 40 del propio Reglamento–, ordena que:

> «[s]olo podrá prestar un servicio cualificado de conservación de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que utilice procedimientos y tecnologías capaces de ampliar la fiabilidad de los datos de la firma electrónica cualificada más allá del período de validez tecnológico».

Esta redacción viene a contener dos requisitos para la prestación del servicio, de corte genérico. Un requisito está referido al empleo de procesos y el otro requisito se refiere a tecnologías que permitan esta ampliación de la fiabilidad de la firma o sello más allá de su periodo de validez tecnológico.

Como se puede ver, el servicio se ordena a resolver un problema estrictamente técnico, en particular referido a la pérdida de seguridad de los algoritmos criptográficos empleados para la firma y sello electrónico cualificado. Por ello el requisito es únicamente disponer de la correspondiente tecnología, y aplicar el correspondiente proceso.

Resulta, sin embargo, criticable que no se establezca ningún requisito respecto a dicha tecnología o al proceso asociado, dado que de esta forma resulta francamente difícil para los operadores jurídicos determinar el alcance de las obligaciones asociadas al servicio.

5.2.2. Especificaciones técnicas

Como en el servicio de validación de firma y sello electrónico cualificado, también en este caso podemos referirnos a las especificaciones y normas técnicas y, en concreto, a la ya menciona norma ETSI EN 319 102-1. Esta norma identifica tecnologías y contiene procesos para la creación y validación de firmas y sellos electrónicos, de forma que se pueda lograr este objeto de ampliación del periodo de validez técnica de estas pruebas electrónicas.

Más en concreto, esta norma, y en relación con las normas de formato de firma y sello electrónico, prevé la posibilidad de crear una clase de firma electrónica que ofrece disponibilidad a largo plazo e integridad de materiales de validación. Ello se logra añadiendo sellos de tiempo electrónico u otras tecnologías a una firma o sello electrónico avanzado. Así, gracias a estos sellos se puede comprobar la validez de una firma o sello incluso aunque haya expirado toda la información necesaria para la validación de los elementos que respaldan la firma. La expiración se produce, bien porque los certificados del prestador del servicio de confianza han expirado, o bien porque se ha producido una pérdida crítica de la fiabilidad de alguno de los algoritmos criptográficos empleados. Esta comprobación de la validez de una firma o sello mediante la adición de sellos de tiempo electrónico u otras tecnologías es una diferencia respecto a la segunda modalidad de proceso de validación.

Sólo cuando nos referimos a la pérdida de fiabilidad de los algoritmos criptográficos podemos hablar, de forma estricta, de conservación más allá del periodo de validez tecnológico de la firma o del sello. Esto es así, dado que el caso de la expiración del certificado que respalda la firma no predica nada acerca de la validez tecnológica de la firma o sello, que puede seguir siendo perfectamente adecuado y seguro. Dicha expiración podrá afectar, en función del caso, a la validez –o más correctamente, a la eficacia– jurídica de la firma o sello electrónico, pero sólo en caso de que no se pueda levantar la carga procesal con respecto a esta prueba electrónica.

De forma correspondiente, la norma ETSI EN 319 102-1 contiene una tercera modalidad del proceso de validación, prevista para la validación de esta clase de firma o sello, por lo que el servicio de validación podrá también procesar estas firmas o sellos electrónicos.

El Reglamento eIDAS no establece más requisitos específicos en relación con este servicio, al que resultan también aplicables los requisitos generales aplicables a los prestadores de servicios de confianza, sin cualificación o con ella.

Una duda importante que plantea este servicio es si el mismo implica que la conservación física del objeto de firma o sello deba correr necesariamente a cargo del prestador, o la pueden realizar el firmante o creador de sellos, o la parte usuaria; es decir, si esta conservación es un requisito del servicio.

A tenor de la dicción literal del Reglamento eIDAS, se puede entender que sería conforme al mismo un servicio que simplemente aplicara el proceso tecnológico previsto en las normas técnicas –por ejemplo, la adición de un sello cualificado de tiempo electrónico de archivo a la firma o sello electrónico cualificado–, devolviendo posteriormente la firma o sello modificada a la persona usuaria del servicio.

En contra de esta posibilidad se podría oponer que la denominación del servicio implica, en efecto, la obligación de conservación del objeto de firma o sello electrónico, pero dicha interpretación parecería excesiva, dado que nada más en el Reglamento la apoya. En este caso, además, seguramente se planteará el debate acerca del rol de las tradicionales instituciones de archivo de documentos.

Más correcto parece la interpretación, que encuentra apoyo en las normas técnicas anteriormente aludidas, en cuya virtud la conservación física del objeto de firma o sello sería una opción técnica más para la ampliación del plazo de validez técnica de dicha firma o sello, alternativa o complementaria a la adición de sellos de tiempo electrónico de archivo, conforme al ejemplo anteriormente expuesto.

Esta interpretación es la que adopta nuestra legislación del sector público, en concreto en la Norma Técnica de Interoperabilidad de Política de firma y de sello electrónicos y certificados de la Administración, aprobada por Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas.

De forma consistente con lo que se acaba de indicar, tampoco es un requisito del servicio proceder a la conservación del documento o mensaje firmado o sellado, aunque ciertamente pueda resultar conveniente; algo que en algún Estado ha supuesto la regulación, en sede nacional, del correspondiente servicio de confianza de archivo electrónico, como en Bélgica.

5.3. Los efectos jurídicos asociados al servicio

Como en otros casos, tampoco en este caso el Reglamento eIDAS establece ningún efecto jurídico expreso y específico para este servicio. A pesar de ello, el servicio produce un innegable efecto jurídico en el ámbito probatorio, facilitando la prueba de la firma o sello electrónico cualificado, en especial cuando haya transcurrido un plazo significativo de tiempo, y en todo caso, cuando se haya puesto en cuestionamiento la seguridad de alguno de los algoritmos en que se basó.

Ello resulta especialmente importante en documentos o mensajes que requieren un largo plazo de conservación, No obstante, hay que tener presente que la necesidad de conservar la firma o sello electrónico encuentra su límite natural en los plazos de prescripción y caducidad de las acciones, dado que puede tener poco sentido mantener el valor de la prueba electrónica cuando ya no se puede generar discusión procesal alguna acerca de la autenticidad de la firma o sello electrónico.

Bibliografía

Alamillo Domingo, I. (2016). «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autenticación de los ciudadanos». En: Gamero Casado, E.; Fernández Ramos, S.; Valero Torrijos J. (eds.) *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (1.ª ed., págs. 675-768). Valencia, España: Tirant lo Blanch.

Martínez Nadal, A. (1998). *Comercio electrónico, firma digital y autoridades de certificación.* Madrid, España: Civitas.

Martínez Nadal, A. (2009). *Comentarios a la Ley 59/2003 de firma electrónica* (2.ª ed.). Cizur Menor: Civitas Thompson Reuters.

Merchán Murillo, A. (2012). «La firma electrónica: Problemas en su reconocimiento transfronterizo». *Revista de Contratación Electrónica* (núm. 117, pág. 3-29).

Merchán Murillo, A. (2016). *Firma electrónica: Funciones y problemática (Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica)* (1.ª ed.). Cizur Menor, Navarra, España: Aranzadi.

Ortega Díaz, J. (2008). *La firma y el contrato de certificación electrónicos* (1.ª ed.). Cizur Menor: Thomson Aranzadi.

Pérez Pereira, M. (2009). *Firma Electrónica: Contratos y Responsabilidad Civil* (1.ª ed.). Cizur Menor, Navarra, España: Aranzadi.

Rodríguez Ayuso, J. F. (2018). *Impacto de la nueva regulación europea sobre identificación electrónica y servicios de confianza en el ámbito de la contratación privada dotada de firma electrónica.* Alma Mater Studiorum - Università di Bologna, Bologna.

Sarwat, R. (2010). *DNI-e. Tecología y usos* (1.ª ed.). Móstoles, Madrid, España: Informática64.