Entorno legal y normativo en organizaciones públicas y privadas

Ignacio Alamillo i Domingo

PID_00195859

UOC
Universitat Oberta de Catalunya

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.

En primer lugar presentamos el concepto de firma electrónica, sus tipologías existentes, el régimen jurídico general y efectos jurídicos correspondientes a cada caso.

En segundo lugar estudiamos los principales aspectos técnicos vinculados con la firma electrónica, como son los algoritmos criptográficos, el uso de las claves y los dispositivos de firma. Dichas nociones son significativas para comprender el funcionamiento y las garantías de los diferentes sistemas de firma electrónica a emplear en cada caso.

En tercer lugar explicamos los certificados electrónicos, que soportan los sistemas de firma electrónica avanzada y reconocida, y que confirman la identidad del firmante. Se estudian los diferentes tipos de certificados que actualmente se encuentran en el mercado, tanto para su uso por parte de los ciudadanos como por las administraciones públicas.

En las dos últimas unidades vemos aspectos prácticos del uso de la firma electrónica en su principal ámbito de uso, que en la actualidad es la administración electrónica, así como las estrategias de conservación a largo plazo de los documentos firmados electrónicamente.

Objetivos

1. Conocer el marco legislativo de los documentos electrónicos en España.

2. Entender las condiciones de validez de los documentos electrónicos, en especial la firma electrónica.

3. Presentar los conceptos de firma electrónica más relevantes.

1. El régimen jurídico general de la firma electrónica

En España, la **Ley 59/2003**, de 19 de diciembre, de firma electrónica (en adelante, **LFE**), regula esta figura y los elementos que le ofrecen soporte, con carácter horizontal al ordenamiento jurídico español, sin perjuicio de otras regulaciones más concretas. Este es el caso de la **Ley 11/2007**, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (en adelante, **LAE**) o de la **Ley 18/2011**, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de justicia (en adelante, **LUTICAJ**), que constituyen leyes especiales en materia de firma electrónica con respecto a la LFE, tanto en lo que respecta a la creación de nuevas tipologías de certificados como al establecimiento de normas concretas sobre el uso de la firma electrónica en el procedimiento administrativo o judicial, respectivamente.

La LFE define la firma electrónica, sus requisitos y efectos, sobre la base de la equivalencia de la firma electrónica con la firma escrita, y de la no discriminación del uso de tecnología para la identificación y acreditación de la voluntad de las personas. Dicha ley regula, además, la actividad de las entidades que ofrecen los servicios necesarios para la existencia de la firma electrónica, y, en concreto, los requisitos de los denominados certificados y de los prestadores de servicios de certificación, dedicando la práctica totalidad de la regulación a esta actividad.

Podemos avanzar que la firma electrónica es un concepto funcional, neutral tecnológicamente. Es decir, se trata de una descripción de funciones que muchas tecnologías pueden realizar. En el caso que nos ocupa, se trata de las funciones tradicionalmente atribuidas a la firma manuscrita, de forma que cualquier técnica electrónica, informática o telemática que nos permita realizar alguna o todas de estas funciones deberá ser calificada como firma electrónica.

Este es el contenido nuclear de una legislación de firma electrónica: la creación de una regla de equivalencia, a partir de la cual emplearemos la firma electrónica en todos los casos en que actualmente empleamos la firma manuscrita, de forma voluntaria u obligatoria, principio que se plasma en el artículo 3 de la LFE.

Esta regla jurídica tiene diversas consecuencias:

- Dado que una firma electrónica es equivalente a una firma manuscrita (y dado que un documento electrónico firmado electrónicamente es equivalente a un documento en soporte físico firmado manuscritamente), no es

necesario modificar todas las leyes para autorizar el uso de la firma electrónica, sino que se puede emplear directamente.

- Es necesario interpretar los requisitos de integridad y autenticidad documental (así como el incorrectamente denominado no repudio), en virtud del cual una persona no puede refutar las declaraciones que ha efectuado a la luz de la normativa de firma electrónica.

- Una firma electrónica, desde la perspectiva jurídica, no aporta más al documento que una firma manuscrita, de modo que deberemos considerar la necesidad de condiciones adicionales, en función del documento, para dar cumplida respuesta a las necesarias garantías de cada procedimiento en que se produzca el acto documentado (de esta forma se plasma, como veremos, en el artículo 4 de la LFE). Y al mismo tiempo, determinados tipos de firma electrónica aportan al documento un grado de seguridad técnica muy superior a la que aporta la firma manuscrita, como veremos en el caso de la denominada firma electrónica reconocida.

- Finalmente, la firma electrónica es válida en sí misma, sin necesidad de su completa verificación por el destinatario, como por cierto sucede también en el caso de la firma manuscrita. En realidad, lo importante será la prueba procesal del documento firmado, que no habrá podido ser manipulado por ninguna parte sin dejar huella de la misma.

Desde la perspectiva del usuario de la firma electrónica, que es la que en este momento nos interesa, resulta necesario comentar solo unos pocos artículos de la LFE:

- El artículo 3, sin duda el más importante, por cuanto define la firma electrónica, el documento electrónico y establece su validez y efectos jurídicos. Este artículo se debe relacionar con la disposición adicional décima, que modifica la Ley de Enjuiciamiento Civil, incluyendo un nuevo párrafo 3 al artículo 326, que se refiere al artículo 3 de la LFE, que también veremos cuando analicemos los efectos de la firma electrónica.

- El artículo 4, que regula el uso de la firma electrónica en el procedimiento administrativo, permitiendo la imposición de condiciones adicionales por parte de la Administración pública que emplee sistemas de firma electrónica.

- Los artículos 15 y 16, que regulan el documento nacional de identidad electrónico, que deberá ser aceptado por todas las personas, físicas o jurídicas, públicas y privadas, como instrumento de identificación y de firma de las personas físicas a las que se suministre.

- El artículo 23, que regula los casos en los que los intermediarios de la firma electrónica no serán responsables jurídicamente, y en concreto, el aparta-

do 4 del citado artículo, que viene a indicar las obligaciones de los usuarios de la firma electrónica.

- Los artículos 24 y 25, referidos a los dispositivos de firma y de verificación de firma electrónica.

- Los artículos 26 y 27, que regulan la certificación del cumplimiento, por los intermediarios, de sus obligaciones legales relativas al suministro del servicio y de los dispositivos seguros de creación de firma a sus clientes.

Por otra parte, desde la perspectiva del prestador de servicios de certificación que expide certificados, resulta necesario conocer todo el resto de la ley, dado que se encarga, precisamente, de la regulación de esta actividad[1].

(1)Esta regulación se aborda solo muy tangencialmente en este trabajo, ya que existe una extensa y notable bibliografía en nuestro país.

1.1. La definición y los niveles de firma electrónica

La LFE, siguiendo la normativa de la Unión Europea, considera diversos niveles de seguridad y, por tanto, de eficacia jurídica potencial, a las tecnologías que se pueden cualificar de firma electrónica:

- La firma electrónica
- La firma electrónica avanzada
- La firma electrónica reconocida

1.1.1. La firma electrónica

De acuerdo con el artículo 3.1 de la LFE, la firma electrónica se define como el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante; es decir, una credencial o documento electrónico que nos identifica electrónicamente.

Esta definición, de corte general, califica como firma cualquier tecnología de identificación, con independencia de su idoneidad como instrumento de declaración volitiva, dado que de lo que se trata es de identificar a una persona, debiendo entender que las tecnologías que no ofrecen ni siquiera esta capacidad de identificación no cabe denominarlas *firma electrónica*.

Se corresponde esta definición con la función más básica que se predica de una firma escrita, que es sencillamente indicar qué persona remite un documento. Algunos ejemplos de la misma son los identificadores y contraseñas de usuario que suministran muchas entidades, públicas pero especialmente pri-

vadas, para realizar operaciones a través de las redes telemáticas; o la inclusión de la firma digitalizada en un documento, al efecto de crear la apariencia de documento firmado.

1.1.2. La firma electrónica avanzada

El artículo 3.2 de la LFE define, a continuación, la firma electrónica avanzada como la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a los que se refiere, y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Esta segunda definición, incremental en requisitos sobre la más general de simple firma electrónica, exige que la tecnología, además de identificar a la persona que remite el documento, permita imputar el documento a la persona que dispone de los mecanismos para producir la firma. Además, a diferencia de la firma manuscrita, la tecnología calificable como firma electrónica avanzada debe garantizar la integridad del documento, de modo que las modificaciones posteriores del mismo sean detectables (como sucede en el mundo del papel con la "tachaduras y las raspaduras").

La definición se corresponde con las funciones tradicionales de la firma manuscrita, de modo que la firma avanzada resulta idónea para que las personas físicas procedan a utilizar dicha tecnología. El ejemplo más habitual de tecnología de firma electrónica avanzada es la firma digital basada en criptografía asimétrica.

Ved también

En la unidad "Cifrado y algoritmos en la firma electrónica" de este mismo módulo, podéis ver los conceptos vinculados a la criptografía.

Por último, cabe decir que una de las principales funciones de la LFE es apuntalar jurídicamente esta asunción de que el mecanismo tecnológico de la firma digital puede actuar "como si fuera" la firma manuscrita de una persona, mediante el concepto –tecnológicamente neutral– de la firma electrónica (avanzada o reconocida).

1.1.3. La firma electrónica reconocida

La LFE contiene, finalmente una tercera definición de firma electrónica en su artículo 3.3, en virtud de lo que se considera firma electrónica reconocida a la firma electrónica avanzada, basada en un certificado reconocido y que ha sido producida mediante un dispositivo seguro de creación de firma electrónica, categoría cuyo reconocimiento se refiere a una presunción de idoneidad que la califica especialmente como equivalente a la firma manuscrita, y sin que ello implique la discriminación de los restantes tipos de firma electrónica.

Se trata, de nuevo, de una definición incremental en cuanto a los requisitos, que exige que la tecnología de firma electrónica reconocida sea especialmente idónea y adecuada para que una persona física, de hecho típicamente un ciudadano o profesional usuario de servicios privados y públicos, se identifique y firme.

1.2. Los efectos jurídicos de la firma electrónica

En este apartado vamos a ver las implicaciones de la firma electrónica a efectos legales. Para ello, en primer lugar tratamos el principio de validez legal de la firma electrónica.

En segundo lugar estudiamos los efectos de la firma electrónica y los principios asociados. A continuación, describimos el concepto legal de documento firmado electrónicamente, aplicable con carácter general a todo el ordenamiento jurídico.

Por último, abordamos la firma electrónica desde la perspectiva de su funcionamiento como prueba judicial.

1.2.1. El principio de validez general de la firma electrónica

Llegados a este punto, no es conveniente seguir sin explicitar una cuestión importante:

Toda firma electrónica, con independencia de su calificación como ordinaria, avanzada o reconocida, es igualmente firma, en la medida en que sirve al objetivo de imputar el contenido del documento a la persona que lo autoriza.

Jurídicamente, toda firma lo es en cuanto se puede imputar a una persona, de acuerdo con las circunstancias concretas del caso, de acuerdo con la situación concreta, que varía en función de las solemnidades y de las formas exigidas

para la producción de cada acto jurídico. En este sentido, el artículo 3.9 de la LFE indica que no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida con relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

La diferencia real entre una simple firma electrónica, una firma electrónica avanzada o una firma electrónica reconocida no reside en su admisibilidad jurídica, ni en su potencial eficacia, sino en el conjunto de requisitos necesarios para lograr dichos efectos.

De esta forma, tenemos que la simple firma electrónica puede no ser idónea, ella sola, para imputar un acto a una persona, de modo que necesitaremos elementos y condiciones adicionales para asegurar la evidencia que ofrece el documento en forma electrónica. Por otra parte, el empleo de la firma electrónica reconocida es el que mayor seguridad jurídica aporta, y el que mejor asegura la efectividad potencial posterior del documento, en la fase probatoria.

En definitiva, hay que tener en cuenta que toda tecnología puede ser empleada como firma, pero que solo una determinada tecnología siempre "es" firma, presunción que facilita el uso de la firma electrónica y genera seguridad jurídica. Sin embargo, una vez determinada la idoneidad de cualquiera de ellas para un caso concreto, resulta que ninguna firma lo es menos que la otra.

1.2.2. La eficacia de la firma electrónica

Respecto a los efectos de la firma electrónica, encontramos un tratamiento de la cuestión aparentemente doble en la LFE, que enseguida veremos que en realidad es el mismo en ambos casos.

Por una parte, el artículo 3.4 de la LFE determina 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; esto es, que la firma electrónica que cumple estos requisitos se "reconoce" legalmente como equivalente a la firma manuscrita.

Por otra parte, el artículo 3.9 de la LFE establece que no se negarán efectos jurídicos a la firma electrónica que no reúna los requisitos de la firma electrónica reconocida, con relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica; esto es, que toda firma puede potencialmente recibir efectos jurídicos, no pudiendo ser ninguna tecnología discriminada por ser electrónica.

Esta concepción doble se traduce en los dos principios generales descriptivos de la eficacia de la firma electrónica: el **principio de no discriminación**, de acuerdo con el 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 era suficientemente fiable como para imputar el acto a la persona

que la produjo; y el **principio de equivalencia funcional**, que no elimina la necesidad de esta prueba, pero la reduce considerablemente, mediante la presunción de la especial idoneidad de la tecnología para actuar como la firma de la persona.

Los efectos, por tanto, se condicionan siempre y en todo caso a la prueba de la autenticidad de la firma, demostrada la cual, la firma producirá su efecto típico, que es el de permitir la imputación del documento firmado a la persona, en los términos de la legislación procesal, sin perjuicio de que, como establece el artículo 3.10 de la LFE, a los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

1.2.3. El documento firmado electrónicamente

De acuerdo con el artículo 3.5 de la LFE, en su redacción por Ley 56/2007, de 28 de diciembre, es documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado, y que, según el artículo 3.6 de la LFE, será soporte de:

- Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la Ley en cada caso.

- Documentos expedidos y firmados electrónicamente por funcionarios o trabajadores públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

- Documentos privados.

El artículo 3.7 de la LFE aclara que los documentos anteriormente referidos tendrán el valor y la eficacia jurídica que corresponda a su naturaleza respectiva, de conformidad con la legislación que les resulte aplicable.

Por su parte, el apartado segundo de la disposición adicional primera de la LFE determina que, en el ámbito de la documentación electrónica[2], corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa.

(2)Una entidad prestadora de servicios de certificación expide certificados de firma electrónica, o presta otros servicios con relación a la firma electrónica.

Cada uno de estos tipos de documentos incorpora la firma electrónica, pudiendo ser firma electrónica ordinaria, firma electrónica avanzada o firma electrónica reconocida, excepto cuando la legislación aplicable establezca un nivel mínimo.

1.2.4. La prueba judicial de la firma electrónica

Es precisamente esta prueba de la autenticidad de la firma electrónica la que hemos de practicar en caso de **repudio** o **rechazo** del documento por parte del demandado, al igual que sucede en el caso de la firma manuscrita, que en caso de conflicto se sustancia mediante una prueba pericial caligráfica.

Al efecto, la LFE determina un tratamiento específico de la prueba de la autenticidad de la firma electrónica, en los casos de la firma avanzada y de la firma reconocida, olvidando –sorprendentemente– la firma electrónica simple u ordinaria. Sin embargo, de nuevo, aunque el tratamiento parece diferente al principio, en realidad es el mismo.

> Determina el artículo 3.8 de la LFE, al efecto, que en caso de impugnarse la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica; así como que la carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida.

Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. E incluso, si a juicio del tribunal la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros, tratamiento similar a la prueba de cotejo de letras.

También determina el mismo artículo 3.8 de la LFE que si se impugna la autenticidad de la firma electrónica avanzada, se deberá estar a lo dispuesto por el artículo 326.2 de la LEC, que permite el empleo de cualquier medio de prueba que resulte útil y pertinente.

A pesar de este doble tratamiento, en ambos casos el tratamiento probatorio va a ser el mismo, en caso de conflicto, ya que se deberá acudir a una prueba pericial informática. Esta prueba podrá simplificarse mediante la aportación, por parte de los prestadores de los servicios de seguridad o de los servicios de certificación de la firma electrónica, o por parte de los fabricantes de la tecnología, de certificados que acrediten que los servicios y los productos empleados cumplen los requisitos de seguridad aplicables al caso concreto. Estos

certificados deben estar conformes a la normativa industrial o conforme a un esquema nacional de evaluación y acreditación de la seguridad de las tecnologías de la información.

En el caso de la firma electrónica reconocida, el contenido de la pericia a realizar se encuentra determinado por la LFE:

- Verificación de que el algoritmo de firma empleado corresponde a un sistema de firma electrónica reconocida.

- Verificación de la condición del dispositivo empleado como seguro.

- Verificación de las prácticas del prestador del servicio que emiten el certificado como reconocido.

En el caso de la firma avanzada no se establece criterio ninguno, dado que en aplicación del principio de neutralidad tecnológica, cualquier tecnología puede ser cualificada como firma electrónica avanzada, haga uso o no de certificados o dispositivos de firma, y por tanto difícilmente puede prever el legislador cómo se debe demostrar que una tecnología concreta no ha sufrido un problema de seguridad que la invalide como firma electrónica avanzada. Esta segunda solución debe resultar también aplicable, en nuestra opinión, a la firma electrónica simple u ordinaria, al objeto de evitar la indefensión de la parte que combate la impugnación por falta de cauce procesal, como de hecho resulta habitual en nuestros tribunales.

Como hemos anticipado, la diferencia que realmente existe entre la prueba de la firma electrónica reconocida y de los restantes tipos de firma electrónica es el grado de definición de los aspectos a comprobar en la pericial informática, que en el caso de firma electrónica reconocida facilita la preparación de la prueba y, en su caso, la anticipación de la misma, y que además establece la presunción de autenticidad de la firma electrónica reconocida una vez verificada, ventaja que deberá tomarse en consideración como criterio de selección del nivel de firma requerido en un acto concreto.

Que no se defina legalmente qué debe formar parte de la prueba pericial informática en los casos de la firma electrónica simple u ordinaria, y de la firma electrónica avanzada no significa que la prueba no sea posible o más compleja, sino que habrá que estar al caso concreto y, especialmente, a la definición de las medidas de seguridad de la concreta tecnología que se va a emplear como firma electrónica.

Para cerrar este marco, la disposición adicional décima de la LFE ha añadido un apartado tercero al artículo 326 de la LEC, que establece que cuando la parte a la que interese la eficacia de un documento electrónico lo solicite o

cuando se impugne su autenticidad, se procederá de acuerdo con el artículo 3 de la LFE, que como hemos visto conecta también con el apartado segundo del artículo 326 de la LEC, en una remisión circular difícil de justificar.

2. Cifrado y algoritmos en la firma electrónica

La firma electrónica, para su seguridad, precisa estar soportada en cifras seguras para su producción y comprobación. Por eso en este apartado vamos a estudiar qué es la criptografía, los algoritmos, las claves, y los dispositivos que permiten la firma electrónica.

2.1. La criptografía y las cifras criptográficas

La criptografía es la ciencia que trata la protección de la información mediante el desorden por transposición o sustitución (*cryptós*) de las letras (*graphós*) de un documento, con el objetivo de hacerlo confidencial. La criptografía se diferencia de la *esteganografía*, que tiene por objetivo esconder la información (*esteganós*) entre las letras (*graphós*) de un documento.

La regulación del uso de la criptografía ha sido relativamente restrictiva hasta tiempos muy recientes, porque muchos estados han considerado la criptografía como una técnica de doble uso (civil y militar) y han impuesto controles y obligaciones exorbitantes tanto a las empresas que producían como a las que trabajaban con criptografía.

Restricciones al uso del cifrado

De hecho, en algunos estados, ha existido o aún existe la obligación de entregar copia de las claves criptográficas de los ciudadanos a las autoridades, sin el necesario control judicial. En este sentido, la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, aún determina en su artículo 36.2 que "el cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente."

La aplicación de la criptografía a las tecnologías de la información y la comunicación se basa en algoritmos y claves correspondientes a las diferentes cifras, simétricas y asimétricas, que se utilizan para operaciones de firma, cifrado o resumen, entre otras.

Por su parte, una cifra es un mecanismo criptográfico para proteger una información (sea una comunicación en tránsito o un documento más o menos perdurable) de forma que los terceros no autorizados no puedan acceder.

Las cifras se basan en el uso de claves para mezclar o sustituir la posición de los signos alfabéticos y numéricos que componen el documento, operación que se denomina cifrar. La clave aporta la información necesaria para devolver el documento, ahora desordenado y por tanto ininteligible, a su estado original, operación que se denomina descifrar.

Las cifras pueden ser simétricas o asimétricas:

- La **cifra simétrica** utiliza una sola clave para cifrar y para descifrar y, en consecuencia, esta clave ha de ser conocida por el originador y por el destinatario de la transmisión o del documento confidencial.
  Las cifras simétricas son muy eficientes y permiten ejecutar operaciones con mucha velocidad, pero el descubrimiento de la clave (o del libro de claves, en su versión más sofisticada) compromete la seguridad de todas las informaciones protegidas con esta cifra.

- La **cifra asimétrica** utiliza dos claves, una para cifrar y otra para descifrar, de forma que ya no es necesario que el originador y el destinatario de la transmisión o del documento confidencial compartan ninguna clave. Las cifras asimétricas son muy seguras, pero no tan eficientes como las simétricas, y además incrementan de forma muy importante el volumen del documento protegido.

2.2. Los algoritmos criptográficos

Los algoritmos que tienen por finalidad el tratamiento del secreto de la información se denominan criptográficos y son esenciales para la firma electrónica, ya que soportan el uso de cifras seguras para la producción y comprobación de la firma electrónica.

Un algoritmo es una función matemática ejecutada por un producto informático, formado habitualmente por un bien de equipo (hardware) y una aplicación o programa (software). Los algoritmos se basan en un problema matemático, cuya dificultad de resolución es lo que lo hace seguro, aunque con el tiempo se puede resolver, aspecto que se debe tener en cuenta. Los algoritmos criptográficos, por tanto, residen en el corazón de la firma electrónica.

Uno de los principales inconvenientes de todos los algoritmos es que cuanto más tiempo transcurre desde su aplicación, mayor es la posibilidad de encontrar un algoritmo que produzca resultados fraudulentos, en especial, debido al incremento progresivo de la capacidad de cálculo.

En definitiva, ello implica que una firma digital creada hoy sea solo segura mientras tanto el algoritmo como la clave empleada no hayan sido superados por la capacidad de cálculo de un atacante. En términos prácticos, se suelen marcar periodos de tiempo durante los cuales se considera seguro el empleo de una cifra, y transcurridos los mismos, resulta necesario preservar la firma electrónica.

El **Centro Criptológico Nacional (CCN)** tiene la misión de actuar como entidad de certificación criptológica. Entre sus funciones está la de evaluar la calidad de los algoritmos generados por los productos informáticos. En relación con la firma electrónica y la administración electrónica, el CCN vela por el uso y la calidad de la criptología en España a través de la publicación de las Guías CCN-STIC-405 y 807, sobre criptografía. Estas guías constituyen excelentes pautas para establecer la política de cada organización en materia criptológica y, más en concreto, para reducir los riesgos de cumplimiento legal.

Centro Criptológico Nacional

El CNN es el organismo responsable de la elaboración del Catálogo de Productos con Certificación Criptológica, que incluye los productos capaces de proteger la información clasificada nacional. De esta forma, tiene la consideración de cifrador nacional, con certificación criptológica aquel equipo de cifra que ha sido evaluado y ha obtenido dicha certificación del CCN. Se dispone de distintos tipos de cifradores: IP, de datos, voz, fax, productores de PKI, generadores de números aleatorios, centros de gestión, etcétera.

En este subapartado veremos con más detalle los distintos componentes criptográficos que intervienen en la firma electrónica: los algoritmos de resumen, y los algoritmos de firma.

2.2.1. Los algoritmos de resumen

El algoritmo de resumen permite obtener una versión reducida de un documento que hay que firmar. Esta versión resumida se puede enviar juntamente con el documento para garantizar que el documento no ha sido manipulado (propiedad que se denomina integridad documental electrónica).

Este sistema se aplica, en relación con la firma electrónica avanzada, porque las operaciones ejecutadas con algoritmos de firma son muy lentas y, adicionalmente, incrementan mucho el volumen del documento firmado. Para evitar estos inconvenientes, lo que realmente se firma es este resumen, y no el documento entero. También hay muchas aplicaciones que requieren la integridad documental, pero no la firma electrónica y, por tanto, también utilizan estos algoritmos de resumen.

El algoritmo de resumen ha de garantizar una serie de condiciones:

- Ha de ser irreversible; es decir, del resumen no se ha de poder obtener el documento original.

- Ha de ser único para cada documento e infalsificable; es decir, no han de existir dos o más resúmenes iguales para documentos diferentes ni dos resúmenes diferentes del mismo documento.

El algoritmo de resumen que habitualmente se utiliza es **SHA-1**, aunque ya se han propuesto como sustitutos habituales SHA-224, SHA-256, SHA-384 y SHA-512, por su mayor fortaleza. En concreto, el algoritmo MD5 ya ha sido declarado obsoleto para bastantes aplicaciones, y el algoritmo SHA-1 se debería haber dejado de emplear antes de finalizar el 2010, de acuerdo con las recomendaciones del CCN-CERT para la firma electrónica reconocida.

CCN-CERT

El CCN-CERT es la capacidad de respuesta a incidentes de seguridad de la información del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI). Este servicio se creó a principios del 2007 como CERT gubernamental español y está presente en los principales foros internacionales, en los que se comparte objetivos, ideas e información sobre la seguridad de forma global.

2.2.2. Los algoritmos de firma

El algoritmo de firma se basa en una cifra asimétrica; es decir, formada por una **clave privada** y una **clave pública**, que permite firmar documentos con la clave privada y verificar la firma con la clave pública.

Ved también

En el apartado "Las claves criptográficas" podéis ver con más detalle la clave pública y la clave privada.

Criptográficamente, firmar es generar un dato matemático asociado al documento electrónico, de la misma manera que en el mundo físico, firmar es producir un grafismo fijado al soporte material que contiene el documento.

Esta firma ofrece también la propiedad denominada **integridad documental electrónica**, que nos permite determinar que un documento no ha sido manipulado, así como la propiedad denominada **autenticación**, que nos permite comprobar cuál ha sido la entidad que ha originado el documento.

La clave de cifra utilizada por el algoritmo de firma se denomina legalmente dato de firma electrónica. En concreto, la clave privada de firma se denomina dato de creación de firma electrónica y la clave pública de firma se denomina dato de verificación de firma electrónica.

El algoritmo de firma ha de garantizar una serie de condiciones:

- Ha de ser irreversible, en un doble sentido; en primer lugar, de la clave pública no se ha de poder obtener la clave privada; en segundo lugar, de la firma no se ha de poder obtener la clave privada.

- La firma electrónica producida debe ser única para cada documento e infalsificable; es decir, a partir de una manipulación del documento original no se ha de poder obtener una firma idéntica a la del documento original.

El algoritmo de firma electrónica que habitualmente se utiliza es RSA con longitud de clave de 1024 bits, si bien la Guía CCN-STIC-405 establece una recomendación fuerte de migración a RSA con longitud de clave de 2048 bits hasta el 2010, y a partir de esta fecha, empleo de ECDSA con longitud de claves de 256 bits.

2.3. Las claves criptográficas

Las claves criptográficas son los elementos numéricos que forman una cifra criptográfica. Estas claves funcionan conjuntamente con los algoritmos criptográficos para generar firmas electrónicas y las formas de autenticación, o para hacer confidencial un documento.

Por este motivo, las claves son los elementos más importantes y críticos de los sistemas de seguridad en general, y de firma en particular: conocer la clave de una persona implica adquirir la capacidad de identificarse o firmar en nombre de otro, de poder acceder a sus datos secretos.

Las claves criptográficas tienen la consideración legal de datos de creación y de verificación de firma electrónica, de acuerdo con los artículos 24.1 y 25.1 de la LFE:

- Los datos de creación de firma electrónica son, de acuerdo con el artículo 24.1 de la LFE, los "datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica"; por tanto, el aspecto de mayor criticidad del sistema, ya que la posesión o el acceso a los datos de creación de firma permite suplantar al firmante. Los datos de creación de firma han de poder ser protegidos contra la utilización indebida por terceros, y en el caso de la firma electrónica reconocida, se generan dentro de un dispositivo seguro de creación de firma, del cual no pueden extraerse nunca, ni copiarse en ningún otro lugar.

- Por su parte, los datos de verificación de firma electrónica son, de acuerdo con el artículo 25.1, los datos (no se dice que hayan de ser únicos, pero lo hemos de entender en este sentido) como códigos o claves criptográficas públicas, que se utilizan (por los terceros destinatarios de comunicaciones y documentos firmados) para verificar la firma electrónica.

La referencia a códigos o claves criptográficas –privadas y públicas– se hace para preservar la supuesta neutralidad tecnológica de la Ley, aunque claramente podemos decir que en este punto la normativa contempla el caso de las cifras criptográficas asimétricas, y sus algoritmos de firma correspondientes.

Consecuentemente el conjunto más importante de medidas de seguridad en materia de firma electrónica, tiene que ver con la correcta generación, protección y gestión de las claves privadas, tanto cuando corresponden a cifras simétricas como cuando corresponden a cifras asimétricas. También de forma coherente con esta necesidad, la regulación más importante en materia de los dispositivos que se consideran seguros para producir firmas electrónicas gira alrededor de la gestión de las claves de los usuarios.

A continuación vamos a ver con más detalle los distintos aspectos relacionados con las claves criptográficas.

2.3.1. La clave criptográfica privada y la clave criptográfica pública

Una clave privada criptográfica es un dato numérico que forma parte de una cifra y que ha de ser absolutamente secreto, porque sirve para autenticarse, firmar o acceder a datos confidenciales.

En las cifras simétricas, como las que se utilizan para la generación de la firma electrónica ordinaria, solo existe una clave, que conocen tanto el firmante como el tercero que recibe el documento firmado. En este caso, ambas partes han de proteger el secreto de la clave.

En las cifras asimétricas, como las que se utilizan para la generación de la firma electrónica avanzada o reconocida, existen dos claves, de las cuales una es privada y la otra pública. Los que firman lo hacen con la clave privada, mientras que los terceros que reciben documentos firmados los verifican con la clave pública, que no es necesario que sea secreta.

De hecho, la idea es que la clave sea lo más pública posible, motivo por el cual se certifica la clave, en asociación con su titular, que posee la clave privada, para que se pueda librar esta clave pública certificada a través de la red Internet y que llegue a cualquier potencial destinatario de documentos firmados.

2.3.2. La correlación entre las claves criptográficas

La correlación entre claves criptográficas es el ligamen matemático que existe entre la clave privada y la clave pública, que permite utilizar una clave para hacer una acción (firmar, por ejemplo) y la otra clave para deshacerla (por tanto, en nuestro ejemplo, verificando la firma).

Como es evidente, sin este ligamen, que es propio de las cifras asimétricas, el sistema no funcionaría. El ligamen, sin embargo, ha de permitir garantizar la seguridad del sistema, de forma que el conocimiento de la clave pública no suponga una amenaza para la clave privada (propiedad frecuentemente denominada irreversible).

En concreto, el artículo 24.3 de la LFE determina que las claves criptográficas producidas o utilizadas por los dispositivos seguros de creación de firma electrónica han de garantizar, de forma razonablemente segura, que no se podrá obtener la clave privada a partir de la clave pública.

2.3.3. La longitud de las claves criptográficas

La longitud de la clave criptográfica es una propiedad de la clave privada, que consiste en el límite superior del espacio numérico de la cifra, y que por tanto determina el número de combinaciones que debería probar un atacante que quisiera adivinar la clave privada.

La longitud de la clave criptográfica se determina en bits; actualmente, se considera que una clave privada de firma electrónica de usuario de 1024 bits ya es razonablemente segura, mientras que la clave privada de un prestador de servicios de certificación habitualmente tiene una longitud de 2048 bits; todo ello sin perjuicio de las recomendaciones del Centro Criptológico Nacional para la firma electrónica reconocida, en su condición de autoridad competente en materia de cifra.

2.3.4. La generación de las claves criptográficas

El procedimiento de generación de claves tiene por objeto la creación de un nuevo valor numérico correspondiente a una cifra criptográfica; es decir, con este procedimiento obtenemos un nuevo par de claves privada y pública, para su uso (y correspondiente certificación de la clave pública) posterior.

En la mayoría de los casos, es el solicitante del certificado el que se genera, él mismo, su par de claves, y después solicita al prestador de servicios de certificación que genere un certificado con sus datos personales y la clave pública. Con este procedimiento, el prestador nunca conoce la clave privada y, por tanto, nunca podrá suplantar la identidad del firmante.

Aun así, también hay situaciones en que el solicitante no dispone de los mecanismos o de la capacidad (o conocimientos) para generar sus claves criptográficas, y entonces lo delega en el prestador de servicios de certificación. El caso más típico en que se produce esta delegación es cuando el prestador suministra al firmante un dispositivo seguro de creación de firma electrónica, ya que las claves son creadas directamente por el dispositivo, que aún se encuentra en poder del prestador. Para proteger, en estos casos, al firmante, el artículo 18.a) de la LFE prohíbe que el prestador de servicios de certificación almacene o copie la clave privada de firma (los datos de creación de firma, en la terminología legal) de la persona a la que haya prestado el servicio.

Por otra parte, el artículo 20.1.e) de la LFE impone que el procedimiento de generación de claves efectuado por el prestador de servicios de certificación, por encargo de su cliente, sea confidencial, así como la entrega posterior de las claves; y prohíbe su almacenamiento.

2.3.5. La protección de la clave criptográfica

Por su importancia, la clave criptográfica privada ha de ser convenientemente protegida por su titular, habitualmente mediante un producto de firma electrónica, que ha de tener la consideración de seguro.

A la protección de la clave hace referencia la propia definición de la firma electrónica avanzada, cuando indica que esta ha sido creada por medios que el firmante puede mantener bajo su exclusivo control (artículo 3.2 de la LFE).

También se hace una referencia explícita al artículo 24.3 de la LFE, cuando se determina que el dispositivo seguro de creación de firma ha de permitir al firmante proteger de forma fiable los datos de creación de firma electrónica para evitar su utilización por parte de terceros (se entiende que no estén debidamente autorizados).

2.3.6. Los datos de activación de la firma

Los datos de activación de la creación de la firma electrónica son los datos que se utilizan para iniciar un proceso de creación de firma electrónica. Aunque no aparecen definidos en la LFE, su existencia y necesidad conecta con la protección de los datos de creación de firma electrónica, ya que con los datos de activación –que son conocidos por el firmante únicamente, o por las personas en quien delegue la creación de la firma– se puede acceder a los datos de creación de firma y activar el procedimiento de generación de la firma.

Precisamente este dato de activación de la creación de la firma electrónica es el mecanismo de protección más habitual de los datos de creación de firma electrónica al que se hace referencia en el artículo 24.3.c) de la LFE. Los datos de creación de firma están constituidos por un dato alfanumérico, que puede tener una longitud variable, y que debería tener como mínimo ocho caracteres, aunque muchas veces coincide con un número de identificación personal de cuatro dígitos.

2.4. Los dispositivos de firma electrónica

Los distintos componentes que posibilitan una firma electrónica segura se generan mediante herramientas tecnológicas específicas. Estas deben basarse en unos criterios de calidad y estándares. En este apartado estudiamos en detalle las características de los dispositivos de creación y verificación de firmas.

2.4.1. Los dispositivos genéricos de creación de firma y los sistemas operativos

Un dispositivo de creación de firma electrónica es un programa o sistema informático (es decir, un producto) que sirve para aplicar los datos de creación de firma, como indica el artículo 24.2 de la LFE. Esta definición conecta la crea-

ción de la firma electrónica con la aplicación (el uso) de los datos de creación de firma, de forma que el poseedor del dispositivo es realmente la persona que puede crear la firma, sea o no el suscriptor del certificado.

Por este motivo, la firma será imputable al suscriptor en la medida en que una persona no autorizada no pueda aplicar los datos de creación de firma, lo que justifica la necesidad de disponer de los datos de activación de la firma electrónica, por poder hacer esta imputación.

Las aplicaciones informáticas de servicios criptográficos se han convertido en los dispositivos más genéricos de creación de firma electrónica, y aunque progresivamente ofrecen un mayor grado de seguridad, difícilmente pueden ser calificados como dispositivos seguros de creación de firma.

2.4.2. Los dispositivos seguros de creación de firma

Un dispositivo seguro de creación de firma electrónica es un dispositivo que, de acuerdo con el artículo 24.3 de la LFE, cumple los siguientes requisitos:

- Los datos utilizados para la generación de la firma electrónica (es decir, la clave privada) pueden producirse solo una vez y asegura razonablemente su secreto.

- Existe una seguridad razonable de que los datos utilizados para la generación de la firma electrónica no se pueden derivar de los datos de verificación de firma (propiedad de irreversibles) o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento (longitud de claves).

- Los datos de creación de la firma electrónica pueden ser protegidos de forma fiable por el firmante frente a su utilización por terceros (datos de activación de la creación de firma).

- El dispositivo no altera los datos o el documento que ha de ser firmado ni impide que este se muestre al firmante antes del proceso de firma.

El dispositivo seguro es uno de los elementos requeridos para obtener una firma electrónica reconocida, directamente equivalente a la firma escrita. Debido a este especial efecto de equivalencia, las normas europeas contienen una interpretación estricta del concepto, que habitualmente conecta con el uso de un elemento de maquinaria o hardware, como por ejemplo una tarjeta criptográfica o un elemento similar, para poder considerar el sistema como dispositivo seguro de creación de firma electrónica.

En concreto, la especificación técnica CEN CWA 14169 ofrece un perfil de protección, escrito de acuerdo con la norma ISO 15408, que determina criterios comunes para la evaluación de la seguridad de las tecnologías de la infor-

mación, para dispositivos seguros de creación de firma electrónica. Es decir, esta especificación técnica contiene el conjunto de medidas de seguridad que deben cumplir las tarjetas de firma electrónica reconocida, como es el caso del DNI-e o de las tarjetas de los abogados colegiados. Por su parte, la especificación técnica CEN CWA 14170 ofrece un conjunto de medidas de seguridad funcional aplicables a las funciones y programas que funcionan conjuntamente con dispositivos seguros de creación de firma electrónica (programas de firma electrónica), para garantizar un nivel apropiado de seguridad.

Desde la perspectiva de la comprobación de los requisitos expuestos anteriormente, los fabricantes o importadores pueden utilizar el mecanismo de la certificación de productos de firma electrónica del artículo 27 de la LFE, dentro del esquema nacional de evaluación y certificación de la seguridad de productos, al frente de cual se encuentra el Centro Criptológico Nacional.

Los dispositivos actualmente certificados como seguros se pueden ver en la página web del portal de criterios comunes, lo cual facilita la verificación por el firmante del cumplimiento de la legislación de firma electrónica por parte de estos productos.

2.4.3. Los dispositivos de verificación de firma

Un dispositivo de verificación de firma electrónica es, de acuerdo con el artículo 25.2 de la LFE, un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

De acuerdo con esta concepción, cualquier poseedor de la clave pública de una persona puede aplicarla para comprobar la validez de la firma electrónica, debiendo además emplear otros elementos que deberá aplicar esta persona para poder completar el proceso de verificación, como por ejemplo, la construcción de una ruta de certificación hasta una raíz fiable, para comprobar la validez del certificado que contiene la clave pública, o la verificación de todos los certificados de la ruta, que comentaremos posteriormente, debido a su especial importancia para la admisión e interoperabilidad de la firma electrónica.

Los dispositivos de verificación de firma deben garantizar que el procedimiento de verificación cumpla una serie de requisitos generales, previstos en las normas técnicas nacionales e internacionales aplicables y, en su defecto, con las especificaciones técnicas voluntarias, como por ejemplo CEN CWA 14171, sobre procedimientos de verificación de firma electrónica.

Desde la perspectiva de la comprobación de los requisitos expuestos anteriormente, los fabricantes o importadores pueden, igual que en el caso de los dispositivos de creación de firma, utilizar el mecanismo de la certificación de productos de firma electrónica del artículo 27 de la LFE.

Asimismo, debido a la importancia de la verificación de la firma, así como a su frecuente complejidad, la legislación administrativa prevé que las administraciones competentes deban tener acceso al menos a alguna plataforma de verificación del estado de revocación de los certificados.

3. Los certificados electrónicos

La firma electrónica se basa, en general, en el empleo de certificados electrónicos, por lo que debemos referirnos a la regulación que de los mismos se realiza en la LFE.

Con carácter general, un certificado electrónico es, sencillamente, un documento electrónico firmado que garantiza, a las terceras personas que lo reciben o que lo utilizan, una serie de manifestaciones contenidas en el mismo. Estas manifestaciones pueden referirse a la identidad de una persona, a la titularidad o posesión de una clave pública –y de la correspondiente clave privada–, a sus autorizaciones (en forma de roles o permisos), a su capacidad de representar a otra persona física o jurídica, a su capacidad de pago, etc.

Como se puede ver, existe una gran cantidad de posibles certificados, de los cuales solo una pequeña parte ha sido regulada legalmente. Esta certificación tiene como finalidad garantizar la identificación y la firma electrónica de las personas físicas y jurídicas, así como, más recientemente, de las administraciones públicas, sus órganos y entidades de derecho público.

En este sentido, el certificado reconocido de clave pública para la identificación y la firma de las personas físicas es el paradigma legal de certificado electrónico, al cual se acaban asimilando los restantes certificados, como sucede en el caso de los certificados de sello electrónico para la actuación automatizada, administrativa o judicial.

También existe una multiplicidad de formatos técnicos de certificados, de los que el certificado X.509v3 y, en concreto, el perfil que del mismo se ha hecho en el IETF (publicado como RFC 5280), es el más importante y habitualmente utilizado, y base para la interoperabilidad. Estos formatos se aplican a situaciones reales para producir diferentes tipos o clases de certificados, de acuerdo con perfiles personalizados de certificados y con políticas concretas de certificación.

IETF

Internet Engineering Task Force - Fuerza de Trabajo de Ingeniería de Internet, el órgano que prepara los estándares de Internet.

En los apartados que siguen explicamos en detalle distintos aspectos de la certificación electrónica: infraestructura de certificación y tipos de certificación.

3.1. La infraestructura de certificados de clave pública

La infraestructura de claves públicas, también frecuentemente identificada por su denominación inglesa (*Public Key Infrastructure*) y por el acrónimo inglés *PKI*, es el sistema técnico, jurídico, de seguridad y de organización que ofrece soporte a los servicios de certificación y de firma electrónica.

Desde la perspectiva de las aplicaciones y de los usuarios de la firma electrónica, este sistema es una infraestructura que ha de existir previamente a trabajar con la firma electrónica. La infraestructura se denomina de claves públicas porque las operaciones de firma y cifrado requieren como elemento fundamental la publicación y la distribución de las claves públicas de los usuarios de los servicios, en forma de certificados electrónicos de clave pública.

Los integrantes de esta infraestructura pueden ser componentes técnicos o entidades que cumplen un rol o prestan diferentes servicios, incluyendo las llamadas autoridades o entidades de certificación, de registro, de sellos de tiempo y de validación.

Las relaciones que se establecen entre estos sujetos determinan la topología de la infraestructura de claves públicas; es decir, la forma y el alcance del sistema de certificación. Por otra parte, las relaciones internas entre las autoridades de certificación y entre estas y los usuarios determinan el modelo de confianza de la infraestructura de claves públicas.

3.2. Certificado de firma electrónica o de cifrado

El **certificado de firma electrónica** es un certificado de clave pública de usuario final que sirve para generar o para verificar firmas electrónicas, mientras que el **certificado de cifrado** también es un certificado de clave pública de usuario final, pero sirve para cifrar y descifrar documentos.

El certificado de firma y el certificado de cifrado se pueden combinar, de forma que un único certificado permita hacerlo todo, pero en este caso hay que tener en cuenta que si el certificado es (legalmente) un certificado reconocido, entonces no puede almacenarse la clave privada, y en caso de que el usuario la pierda, resulta que ya no podrá descifrar los documentos cifrados, pudiendo perder informaciones y, por ello, sufrir daños.

Esta problemática no existe en los certificados de firma, ya que, aun en caso de perderse la clave privada, se pueden verificar todas las firmas que se generaron con dicha clave, que son igualmente válidas.

Para evitar el riesgo de pérdida de la clave de cifrado, en muchas ocasiones se expiden dos certificados diferentes, y se almacena, en un entorno seguro, una copia de esta clave privada correspondiente al certificado de cifrado. De este modo, si el usuario la pierde, se puede recuperar posteriormente, mediante el correspondiente procedimiento.

3.3. Certificado de firma electrónica ordinario o reconocido

Desde una perspectiva legal, el artículo 6 de la LFE define el certificado de firma electrónica como un documento firmado electrónicamente por un prestador de servicios de certificación, que vincula unos datos de verificación de firma

a un firmante y confirma su identidad, sin establecer ninguna definición para los certificados de otras funcionalidades (como el cifrado), que por tanto quedan sin regulación directa.

Este primer tipo de certificado de firma electrónica se denomina **certificado ordinario** para diferenciarlo del **certificado reconocido**[3].

(3)Una traducción ambigua del término *original* de la Directiva 99/93/CE, de 13 de diciembre, de Firma Electrónica, que quizá se debería haber traducido como 'certificado cualificado'.

Los certificados reconocidos son, de acuerdo con el artículo 11.1 de la LFE, los certificados electrónicos emitidos por un prestador de servicios de certificación que cumple los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y el resto de circunstancias de los solicitantes, y a la fiabilidad y las garantías de los servicios de certificación que prestan.

Todos los certificados ordinarios y reconocidos son, de acuerdo con estas definiciones legales, certificados de clave pública y de usuario final. Es curioso ver cómo la Ley española –al igual que la Directiva europea– deja fuera del concepto legal de certificado (ordinario o reconocido) cualquier certificado de clave pública que no sea de persona o que no sea de identidad o de firma electrónica, como es el de cifrado o el de componente técnico, por lo que dichos certificados son expedidos por los prestadores con sujeción solo a su contrato.

En cualquier caso, el certificado reconocido es una pieza fundamental para la firma electrónica reconocida, y por este motivo la LFE regula con detalle su contenido y los procedimientos y las garantías para emitirlo. Por otro lado, el certificado ordinario, al ser de menor importancia, su regulación es menor: no se regula su contenido, y solo se establecen unas obligaciones comunes –típicamente informativas y de publicación de información– a todos los prestadores que expiden certificados.

En concreto, el certificado reconocido deberá contener, de acuerdo con el artículo 11.2 de la LFE, lo siguiente:

- La indicación de que el certificado se expide como reconocido.
- El código identificativo único del certificado.
- La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
- La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- La identificación del firmante, en el caso de personas físicas, por su nombre y apellidos y por el número de documento nacional de identidad o mediante un seudónimo que conste como tal de manera inequívoca y, en

el caso de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

- Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

- El inicio y finalización del período de validez del certificado.

- Los límites de uso del certificado, si se prevén.

- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

De acuerdo con el artículo 11.3 de la LFE, los certificados reconocidos podrán contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función de la finalidad propia del certificado y siempre que lo solicite el firmante, lo cual permite profundizar en la caracterización de los tipos de certificados reconocidos:

- Los certificados para actuar en nombre propio o por representación.
- Los certificados individuales y los certificados corporativos.

3.4. Certificado para actuar en nombre propio o por representación

El certificado de firma puede servir para actuar en nombre propio o en representación de una persona, como determina el artículo 6.2 de la LFE, al definir la figura del firmante, que puede actuar "en nombre propio o de una persona física o jurídica, a la que representa".

Aunque el caso más habitual en estos momentos es el certificado para actuar en nombre propio, cada vez serán más importantes los certificados que incorporen la representación de un tercero, que, de acuerdo con el artículo 11.3 de la LFE, deberá declarar que su finalidad específica es, además de la identificación de las personas que los reciben, la de actuar por representación: se trata, pues, de un certificado específico, de representante, cuyo uso permitiría la simplificación del procedimiento, administrativo o judicial, en el cual dejaría de resultar necesaria la aportación del clásico apoderamiento.

El artículo 11.4 de la LFE determina que el certificado reconocido como representante deberá incluir una indicación del documento público que acredite de forma fehaciente las facultades del firmante –que es suscriptor del certificado individual, y del poseedor de claves del certificado corporativo– para actuar en nombre de la persona o entidad a la que representa y, cuando sea obligatoria la inscripción de los datos del registro público, de conformidad con el

apartado segundo del artículo 13 de la LFE (parece que esta referencia hay que entenderla hecha al apartado tercero del artículo 13, que es el que realmente trata esta cuestión).

En términos prácticos, un certificado de representación que no incorpore límites de actuación realmente manifiesta que el representante puede llevar a cabo cualquier acto en nombre de su representado, bien por tratarse de un representante legal (orgánico, en el caso de las personas jurídicas representadas), bien por tratarse de un representante voluntario con apoderamiento general.

3.5. Certificado individual o corporativo

El certificado personal puede ser individual cuando lo solicita una persona física, jurídica o entidad sin personalidad, para su uso en nombre propio o por cuenta de tercero, sin indicar una relación de vinculación con otra persona, como trabajador o similar; el modelo de certificado en que se construye el régimen de relaciones jurídicas de la LFE, y que se corresponde con la prestación de servicios al consumidor (al público).

Aunque no aparece citado expresamente, el certificado personal también puede ser corporativo, cuando indica una relación de vinculación de esta naturaleza con otra persona, o una condición profesional vinculada a una corporación colegial, que se pueden incluir entre los contenidos del certificado si lo justifica la finalidad específica del certificado (artículo 11.3 de la LFE).

Habitualmente, el certificado corporativo nace de una relación laboral o de una relación orgánica de pertenencia a una corporación pública o privada, y se diferencia del certificado individual en que la suscriptora del certificado será la corporación, mientras que la persona signataria que lo recibe será considerado como poseedor de la clave de firma, debidamente autorizado para utilizarla de acuerdo con sus facultades, permisos y privilegios indicados en el certificado.

Por lo que respecta a la LAE, su artículo 19 se refiere a la identificación y autenticación del ejercicio de la competencia de la Administración pública, órgano o entidad actuante, la cual se hará mediante firma electrónica del personal a su servicio.

A estos efectos, cada administración pública puede proveer a su personal de firma electrónica, con los efectos que deriven del tipo de firma que se atribuya y con relación al trámite o procedimiento de que se trate, valorándose igualmente si nos movemos en entornos abiertos o cerrados.

La expresión *personal al servicio de las administraciones públicas* debe ser entendida, en nuestra opinión, en un sentido amplio, incluyendo a los órganos o cargos, a los empleados públicos e incluso a otras personas que prestan servicios a las administraciones públicas.

Las ventajas de la certificación corporativa se muestran en toda su plenitud en el caso de los certificados de personal al servicio de las administraciones públicas, puesto que la organización pública, en cuanto suscriptora de los citados certificados corporativos, ostenta unas facultades importantes de solicitud, suspensión, revocación e incluso recuperación de las claves de cifrado del personal (nunca de firma, ya que su archivo y recuperación se encuentran legalmente prohibidas) que no puede tener jamás en el caso de los certificados de ciudadanos, como veremos que también sucede en el caso de emplear el DNI electrónico en el puesto de trabajo.

Ejemplo

Algunos ejemplos prácticos de certificados de personal al servicio de las administraciones públicas, en ambos casos con diez años de servicio continuado, son la T-CAT de CAT-Cert, un dispositivo seguro de creación de firma electrónica que incorpora certificados de identificación y firma, y de cifrado, con recuperación de claves de cifrado, o las diferentes modalidades de tarjeta SCA de órgano, empleado público y corporación, suministradas por IZENPE a las administraciones públicas vascas.

CAT-Cert

La Agència Catalana de Certificació nace en el año 2002 como organismo autónomo del Consorci Administració Oberta de Catalunya. http://www.catcert.cat/esl/.

IZENPE

Empresa de certificación y servicios: Es una sociedad anónima constituida en el año 2002 y supone un proyecto impulsado por el Gobierno Vasco y las Diputaciones Forales. Constituida a través de sus sociedades informáticas: EJIE, LANTIK, IZFE y CCASA. http://www.izenpe.com/s15-12010/es/.

El empleo del DNI electrónico para la autenticación del personal al servicio de la Administración

El artículo 19.3 de la LAE indica que la firma electrónica basada en el documento nacional de identidad podrá utilizarse a los efectos de identificar y autenticar al funcionario.

Esta previsión es criticable, ya que el DNI identifica, pero en ningún caso puede atribuir por sí mismo la condición de funcionario o personal al servicio de las administraciones públicas del que la utilice, por lo que, en la práctica, se puede producir una rebaja de las garantías respecto al procedimiento presencial (en contra de la letra f del artículo 4 LAE).

Algunas limitaciones del uso del DNI electrónico como sistema de firma electrónica del personal al servicio de las administraciones públicas son las siguientes:

- Se trata de un instrumento de ciudadano, que no acredita en ningún caso la condición de órgano o de empleado, dado que no contiene ninguna información relativa a la Administración pública.
- Aunque disponer del DNI-e como soporte físico es obligatorio, no se puede obligar al ciudadano a disponer de certificados, de forma que las funciones de firma electrónica y de identificación son voluntarias, lo que supone que la Administración pública no puede obligar al trabajador a identificarse electrónicamente ni a firmar.
- No dispone de certificados de cifrado, inhibiendo funcionalidades requeridas en el funcionamiento ordinario del procedimiento (en especial cuando se gestionan datos personales de cierto nivel de sensibilidad).
- No permite personalizaciones ni cargar aplicaciones adicionales.
- No permite el control del ciclo de vida de la tarjeta, ni el establecimiento de medidas sancionadoras para caso de mal uso en el entorno corporativo (no se puede incautar, por ejemplo).

Quizá por todos estos límites la propia Policía Nacional, que emite el DNI-e, se ha dotado recientemente de una tarjeta corporativa (denominada carné profesional) para su personal, regulada por Orden INT/761/2007, de 20 de marzo, actuación que lleva a pensar en la poca viabilidad práctica del empleo del DNI-e como tarjeta de empleado público.

3.6. Certificado de sello electrónico para la actuación automatizada

El sello electrónico de Administración, órgano o entidad de derecho público se recoge en el artículo 18 de la LAE, bajo la rúbrica **sistemas de firma electrónica para la actuación administrativa automatizada**.

Por su parte, el artículo 19.1 de la LUTICAJ regula el sello electrónico de la oficina judicial, también bajo la rúbrica de **sistemas de firma electrónica para la actuación judicial automatizada**, en claro paralelismo con la LAE.

En ambos casos, se sigue la regla general de exigir la **identificación y la autenticación del ejercicio de la competencia**, exigible en toda actuación y que, en la automatizada, se puede llevar a cabo mediante dos sistemas:

a) Sello electrónico del órgano administrativo o judicial actuante, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado al órgano actuante y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Resulta criticable la defectuosa inclusión del sello dentro de los sistemas de firma electrónica por simple y directa contradicción entre sello y firma, que evidentemente son conceptos incompatibles.

Y es que resulta necesario considerar los problemas de la aplicación de la legislación vigente en materia de firma electrónica, al caso particular del **sello de actuación automatizada**, puesto que, aunque no puede considerarse que un sello de órgano sea una firma electrónica (ni avanzada, ni reconocida, porque sencillamente es una institución nueva y completamente diferente a la firma), el artículo 18 de la LAE y el artículo 19 de la LUTICAJ determinan que el sello electrónico debe estar "basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica".

Esta manifestación, que parece ciertamente contradictoria, genera algunos problemas de aplicación práctica, ya que la normativa de firma electrónica está orientada a la documentación electrónica de los actos jurídicos por personas físicas, por lo que puede resultar complejo determinar su aplicación directa.

La aplicación de la Ley de Firma Electrónica a los sellos de actuación automatizada

Como ejemplos particulares de problemas a resolver, podemos citar los siguientes:

- La necesidad o no de emplear un dispositivo seguro de creación de sello (por aplicación analógica de la necesidad de empleo de dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24 LFE).

- El tratamiento de los límites de uso de los certificados de sello de órgano, posibilidad que nos parece, más que conveniente, absolutamente necesaria para evitar posibles abusos del sello, especialmente en caso de robo del mismo.

- El tratamiento de la representación legal que ostentan determinados órganos, que en el caso del sello quizá debería limitarse de forma expresa.

Respecto a la creación de los sellos, los artículos 19.1 del RDLAE, en el ámbito de la Administración General del Estado, y 20.1 de la LUTICAJ, en el ámbito de la Administración de justicia, establecen la necesidad de proceder a la creación de los sellos electrónicos mediante resolución, que se publicará en la sede electrónica correspondiente y en la que deberá constar o siguiente:

a) Organismo u órgano titular del sello que será el responsable de su utilización, con indicación de su adscripción en la Administración u organismo público dependiente de la misma.

b) Características técnicas generales del sistema de firma y certificado aplicable.

c) Servicio de validación para la verificación del certificado.

d) Actuaciones y procedimientos en los que podrá ser utilizado.

Como se puede ver, el contenido del acto administrativo de creación del sello persigue la concreción de una serie de contenidos mínimos en relación con el sello correspondiente. En particular, se pueden apreciar dos reglas de corte administrativo, en los apartados a) y d), orientadas a la determinación del titular del sello y de las actuaciones en que se puede emplear; y dos reglas más bien técnicas, en los apartados b) y c), que resultan necesarias dada la insuficiencia de la remisión a la LFE que realizan tanto la LAE como la LUTICAJ.

En efecto, en aplicación del **principio de neutralidad tecnológica**, pueden emplearse sistemas técnicos muy diversos de firma digital, incluso dentro del concepto de sistema basado en certificado, así como diversas sintaxis para el citado certificado, por lo que en algún momento se debe concretar el que se emplea de forma efectiva, a fin y efecto de que sea conocido por la ciudadanía, que en el fondo es la destinataria de las actuaciones administrativas realizadas de forma automática.

La indicación del servicio de validación para la verificación del certificado viene a ser similar, en este caso, en atención a la necesidad ineludible de comprobación del certificado de sello por parte del ciudadano.

La regla referida a la determinación de las actuaciones para las cuales se autoriza el empleo del sello electrónico supone una mitigación del problema de establecimiento de límites en el empleo del sello.

Puede resultar más conveniente disponer de diversos sellos para órganos diferentes, de uso especializado, que de un único sello para toda la Administración y que eventualmente se pueda emplear para cualquier uso.

Asimismo, los artículos 19.2 del RDLAE y 20.2 de la LUTICAJ regulan, con carácter de mínimos, los contenidos del certificado de sello electrónico, incluyendo:

a) Descripción del tipo de certificado, con la denominación de sello electrónico.

b) Nombre del suscriptor.

c) Número de identificación (fiscal o judicial, según corresponda).

Resulta interesante ver que en estos contenidos mínimos solo se considera la identidad del suscriptor, pero no de la persona titular del órgano, posibilidad que prevé la legislación. Es una orientación acertada, dado que en caso de incluirse los datos personales del titular del órgano, se pueden plantear diversos problemas, como la necesidad de revocar el certificado de sello en caso de cese del titular, o una exposición innecesaria de los datos personales de dicha persona al público.

4. El empleo de la firma electrónica en la administración electrónica

Presentada la regulación general de la firma electrónica en nuestro ordenamiento, procede realizar algunas precisiones en cuanto al régimen de uso de la firma electrónica en la administración electrónica; esto es, la LAE y la LUTICAJ, en sus ámbitos respectivos.

4.1. Las condiciones adicionales para el uso de la firma electrónica en la Administración

La LFE dispone, en su artículo 4, determinadas especialidades en el uso de la firma electrónica en la Administración.

Su apartado 1 dispone que:

> "esta ley se aplicará al uso de la firma electrónica en el seno de las administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquellas y estos entre sí o con los particulares",

Una norma que, en puridad, no parecería necesaria, atendido el fundamento competencial de la LFE en el artículo 149.1 de la Constitución Española, competencias 8.ª, 18.ª, 21.ª y 29.ª, y que hoy ha sido complementada y ampliada de forma importante por la LAE y la LUTICAJ.

Es cierto, sin embargo, que la LFE no determina su ámbito subjetivo de aplicación más allá de los prestadores de servicios de certificación, ignorando a los propios usuarios de los servicios, lo cual puede generar problemas importantes, en particular en el ámbito de la ley aplicable en caso de transacciones con elemento internacional.

Tras esta declaración genérica de sujeción a la LFE, el segundo párrafo del apartado 1 del artículo 4 de la LFE concreta que:

> "las administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados".

Las condiciones adicionales, como se puede rápidamente intuir, suponen una alteración importante del régimen liberal de uso de la firma electrónica, y exigen un adecuado tratamiento para cumplir su objetivo declarado, y no convertirse en un elemento de distorsión del mercado.

4.1.1. La caracterización jurídica de las condiciones adicionales

Las condiciones adicionales se configuran legalmente, siguiendo la DFE, como restricciones potenciales a la libre prestación y circulación de servicios de firma electrónica, por lo que resulta necesario limitar el uso de esta posibilidad, y así lo hace el legislador en el apartado 2 del artículo 4 de la LFE, disponiendo que:

> "las condiciones adicionales a las que se refiere el apartado anterior solo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común",

La justificación jurídica de la citada restricción se encuentra efectivamente en el interés superior que representa el procedimiento administrativo, y que exige garantías adicionales a las mínimas que puede ofrecer un mercado con calidades muy diversas.

Además siguiendo a la DFE fielmente, el apartado 2 del propio artículo 4 de la LFE continúa diciendo que:

> "estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo",

Esta regla ha sido, sin embargo, interpretada de forma ciertamente amplia por los Estados miembros de la Unión Europea, lo cual ha afectado a la realización de la promesa de libre circulación de servicios y a la competencia efectiva.

La firma electrónica en los trámites transfronterizos

Resulta especialmente importante resaltar la aparición, en tiempos recientes, de normativa de la Unión Europea especialmente enfocada al uso transfronterizo de la firma electrónica, en particular la Directiva 2006/123/CE, relativa a los servicios en el mercado interior, a partir de la cual la Comisión ha dictado dos Decisiones de extraordinaria importancia:

- La Decisión 2011/130/EU, de 25 de febrero del 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, relativa a los servicios en el mercado interior.

- La Decisión de la Comisión 209/767/CE, de 16 de octubre del 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las "ventanillas únicas" con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior, modificada por la Decisión de la Comisión 2010/425/UE, de 28 de julio del 2010, por la que se modifica la Decisión 2009/767/CE en lo relativo al establecimiento, el mantenimiento y la publicación de listas de confianza de proveedores de servicios de certificación supervisados o acreditados por los Estados miembros.

La importancia de estas Decisiones, especialmente en cuanto ahora nos interesa, radica en la determinación de un conjunto de requisitos que obligan a los Estados miembro a admitir, en cuanto destinatarios de documentos electrónicos, el uso de los sistemas de firma electrónica allí descritos.

Al tiempo, dichos requisitos podrán constituir condiciones adicionales a la utilización de la firma electrónica en el procedimiento, de carácter general sin que sobre las mismas se puedan plantear inicialmente dudas de conformidad o compatibilidad con el Derecho europeo, al menos dentro de su ámbito de aplicación. En efecto, si el propio Estado

miembro queda sujeto como usuario a estas condiciones adicionales, no parece que su extensión a los ciudadanos, en el mismo ámbito de aplicación, sea problemático.

Respecto a la aprobación de las condiciones adicionales, el artículo 4.3 de la LFE prevé que:

"las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica", texto que se habría visto afectado por el artículo 23.3 del RDLAE. Este artículo indica que "las condiciones generales adicionales a que se refiere el artículo 4.3 de la Ley 59/2003, de 19 de diciembre, se aprobarán mediante real decreto aprobado por el Consejo de Ministros a propuesta conjunta de los Ministerios de la Presidencia y de Industria, Turismo y Comercio, previo informe del Consejo Superior de Administración Electrónica".

Esta previsión es interesante porque el apartado 1 del propio artículo 23 del RDLAE indica que:

"los prestadores de servicios de certificación admitidos deberán cumplir las obligaciones de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, así como las condiciones generales adicionales a que se refiere el apartado 3",

ampliando de forma importante las posibilidades de limitar el derecho de admisión previsto en el artículo 21.1 de la LAE.

Nada se dice acerca de la aprobación de condiciones adicionales, generales o particulares, por parte de otras administraciones públicas, ni tampoco respecto de la aprobación de condiciones adicionales particulares por los órganos u organismos de la Administración General del Estado. Cabe pensar, en cualquier caso, que esta posibilidad resulta plenamente posible, excepto cuando el procedimiento venga regulado por normas imperativas de la Unión Europea, como sucede en el caso de la Directiva de Servicios; y que el instrumento normativo apropiado sería el reglamento, atendido el efecto de restricción que supone para los ciudadanos la limitación de uso de posibilidades tecnológicas perfectamente legítimas, pero que la Administración no considera adecuadas para un concreto procedimiento administrativo.

Finalmente, el apartado 4 del artículo 4 de la LFE indica que:

"la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica".

4.1.2. La verificación del cumplimiento de las condiciones adicionales

Para la verificación del cumplimiento de las condiciones adicionales se ha previsto, en el artículo 23.3 segundo párrafo del RDLAE, que:

"corresponde a los Ministerios de la Presidencia y de Industria, Turismo y Comercio [...] controlar el cumplimiento de las condiciones generales adicionales que se establezcan."

La norma resulta excesivamente parca en cuanto a la determinación del régimen jurídico referido a esta actividad de control. Dado que el Ministerio de Industria, Energía y Turismo es el competente para la supervisión general de los prestadores de servicios, parece adecuado que extienda su actividad al control de estas condiciones generales adicionales. Mayores dudas ofrece, sin embargo, la determinación de las actuaciones de control que podrá realizar el Ministerio de Hacienda y Administraciones Públicas, en especial en caso de posibles infracciones a las mismas.

Como alternativa, se podría haber establecido un sistema de certificación de la actividad del prestador de servicios de certificación, que en el artículo 26.1 LFE se define como:

> "un procedimiento voluntario en virtud del cual una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica el reconocimiento del cumplimiento de los requisitos específicos requeridos en la prestación de los servicios que ofrece al público."

Este procedimiento no es único, ya que la expedición de la certificación la puede realizar una entidad acreditada en el marco de la Ley de Industria, pero también puede certificar una entidad sin ninguna acreditación. El artículo 26.2 LFE así lo admite, al referirse, entre otros, a la certificación que llevan a cabo las entidades de certificación reconocidas (más correctamente, acreditadas) por las entidades de acreditación designadas de acuerdo con la Ley de Industria.

Modalidades de certificación de la actividad de los prestadores que expiden certificados

Debemos distinguir por lo menos dos grados o niveles de certificación de la actividad del prestador de servicios de certificación:

- La certificación del servicio por una entidad de certificación acreditada de acuerdo con la Ley de Industria y la normativa de desarrollo posterior.
- La certificación del servicio por otras entidades, de acuerdo con otros criterios, y que ofrece unos beneficios inferiores al anterior.

El primer grado se corresponde con la certificación prevista en el capítulo III del Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y la seguridad industrial (BOE núm. 32 de 06/02/1996), que regula la infraestructura acreditable para la calidad.

El segundo grado se corresponde con la definición de unos requisitos y con la ejecución de una auditoría del prestador de servicios de certificación. Esta auditoría se puede ejecutar por una entidad auditora y de inspección acreditada de acuerdo con el Real Decreto 2200/1995, o por una entidad sin ninguna acreditación dentro del sistema público, posibilidad que ofrece inferiores garantías formales, pero que favorece más la autorregulación de la industria.

Ambas opciones se pueden considerar sistemas voluntarios de acreditación de acuerdo con la Directiva 99/93/CE, de 13 de diciembre, de Firma Electrónica, en función de la voluntad de cada Estado miembro de la Unión Europea, según estos sistemas voluntarios se encuentren alineados con la normativa industrial o, por el contrario, permitan un grado inferior de control público de la actividad de certificación de la actividad de los prestadores de servicios de certificación de firma electrónica.

La ventaja de un **sistema voluntario de certificación** de la actividad es que se puede adaptar a las necesidades de cada escenario al que se aplica, como por ejemplo la administración electrónica, o la administración electrónica de justicia. Sin embargo, quizá por influjo de la regulación europea sobre la ven-

tanilla única, contenida principalmente en la Decisión 2009/767/CE de 16 de octubre del 2009, modificada por la Decisión 2010/425/UE de 28 de julio, así como en la Decisión 2011/130/EU, no parece que esta posibilidad se vaya a desarrollar, puesto que podría entrar en colisión con las obligaciones de los Estados allí establecidas.

En caso de existir un sistema voluntario de certificación de la actividad de los prestadores, no debería interferir con la publicación y aceptación de los certificados expedidos por prestadores supervisados pero no certificados. Es más, no resultaría aceptable en ningún caso, legislación comunitaria en mano, establecer la obligación jurídica de solicitar y obtener la certificación, pero no es menos cierto que facilitaría a los prestadores la verificación previa del cumplimiento de dichas condiciones y, por tanto, aportaría seguridad jurídica y confianza en el uso de la firma electrónica.

4.2. El derecho de admisión de la firma electrónica en el procedimiento

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante, LRJ-PAC) dispone en su artículo 45.5 que los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las administraciones públicas, o los que estas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad e integridad.

El artículo 13.1 de la LAE determina que:

> "las administraciones públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos".

Y concreta el apartado 2 del propio artículo 13 de la LAE, que:

> "los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las administraciones públicas, de acuerdo con lo que cada Administración determine:
>
> a) En todo caso, los sistemas de firma electrónica incorporados al documento nacional de identidad, para personas físicas.
>
> b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las administraciones públicas.
>
> c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen."

Por lo que respecta a la administración electrónica de justicia, el artículo 230 de la LOPJ, en su redacción por Ley Orgánica 16/1994, de 8 de noviembre, autoriza el uso de cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones, con el límite de la legislación de protección de los datos de carácter personal; en consonancia, determina que los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales, en línea con el principio general de proporcionalidad y seguridad.

Por su parte, el artículo 14.1 de la LUTICAJ concreta que:

> "la Administración de justicia admitirá, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y resulten adecuados para garantizar la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos".

Estos sistemas se concretan, como en la LAE, en el apartado 2 del propio artículo 14 de la LUTICAJ, que indica que:

> "sin perjuicio de lo dispuesto en los artículos 4 y 6 de la presente Ley y en todo caso, con sujeción estricta a lo dispuesto por las leyes procesales, los ciudadanos y profesionales del ámbito de la justicia podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con la Administración de justicia:
>
> a) Los sistemas de firma electrónica incorporados al documento nacional de identidad, para personas físicas.
>
> b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las administraciones públicas.
>
> c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen."

La admisión de la firma electrónica es una verdadera obligación para la Administración

Nótese, tanto en la LAE como en la LUTICAJ, el empleo de la forma imperativa del verbo *admitir*, en línea con el derecho de ciudadanos y, en su caso, profesionales al uso de los sistemas de firma electrónica, que no constituye, pues, una decisión discrecional o de concesión graciable por la Administración, sino una verdadera obligación jurídica, exigible siempre que se cumplan las condiciones legales establecidas en la normativa aplicable. El legislador de la LAE y de la LUTICAJ podría haber empleado otros verbos menos exigentes, si no hubiese querido imponer una verdadera obligación a la Administración.

Por otra parte, tratar la admisión de sistemas de firma electrónica como una cuestión puramente discrecional afectaría a las legítimas expectativas de las personas adquirentes de sistemas de firma electrónica basada en certificados, expectativa que deriva directamente de la LFE, y podría dar lugar a potentes distorsiones del mercado, como había venido sucediendo con la admisión exclusiva del certificado de la FNMT-RCM en las relaciones con la AEAT y otras entidades públicas, que venía a apoyar –seguro que de forma involuntaria por los gestores públicos correspondientes– un monopolio *de facto* prohibido por el derecho comunitario y la legislación española.

Es cierto que el artículo 13.2 de la LAE parece matizar la obligación de admitir los sistemas de firma electrónica que se contiene en el apartado 1 de ambos artículos, por cuanto indica que "los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica [...], de acuerdo con lo que cada administración determine", pero no tiene por qué implicar que la decisión de admitir o no un sistema de firma electrónica sea puramente discre-

cional de cada administración, dado que ello implicaría vaciar de contenido el derecho reconocido en el artículo 6.2.h) de la LAE, y artículos 4.2.f) y 6.2.d) de la LUTICAJ.

FNMT-RCM

Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda.

AEAT

Agencia Estatal de Administración Tributaria.

En ambas leyes resulta llamativo que ningún tratamiento privilegiado quede garantizado en relación la admisión de la firma electrónica reconocida, a pesar de que la LFE la configura como la única firma electrónica directamente equivalente a la firma manuscrita, con el valor probatorio reforzado derivado de la presunción establecida por la Ley, y justamente en el momento en que se empieza a disponer de un volumen masivo de unidades de DNI electrónico, que es precisamente una firma electrónica reconocida.

De hecho, sí que puede indicarse que el DNI electrónico recibe un tratamiento privilegiado, derivado de la obligación general de aceptación del mismo que ya se contenía en el artículo 16 de la LFE, y que se plasma en la no necesidad de admisión previa del mismo. Las referencias que se realizan en los artículos 13.2.a) de la LAE y 14 de la LAE a que el DNI electrónico se podrá utilizar "en todo caso y con carácter universal" resultan bastante reveladoras de la voluntad del legislador, en detrimento de las restantes firmas electrónicas reconocidas, que en la LFE reciben el mismo valor y efectos jurídicos que el DNI electrónico.

Se trata de un cambio importante en la orientación de la cuestión hasta la fecha, derivada principalmente de la aplicación de los principios de seguridad y proporcionalidad que informan la LAE y la LUTICAJ, y que obliga a replantear gran parte del debate sobre los tipos y niveles de firma electrónica adecuados para cada procedimiento, pasando de la exigencia de la firma electrónica reconocida en base al principio de estricta equivalencia funcional, a la necesidad de realizar un análisis de riesgo para establecer el nivel de equivalencia material entre el procedimiento presencial existente y su versión electrónica.

4.2.1. La admisión de sistemas de firma electrónica basada en certificados

En el ámbito de la administración electrónica, la admisión de los sistemas de firma electrónica se ha previsto, con carácter general, con relación a aquellos sistemas que se basan en certificados electrónicos. En este sentido, la LAE y la LUTICAJ autorizan el empleo por los ciudadanos de los sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las administraciones públicas.

Desde luego llama la atención la generosidad con la que el legislador de la LAE y la LUTICAJ parecen estar dispuestos a admitir los sistemas de firma electrónica, aspecto con el que nos encontramos, en principio, de acuerdo, dado que

con ello se preserva la neutralidad tecnológica. Además, la referencia expresa a la posibilidad de admitir sistemas basados en certificado electrónico reconocido, aunque innecesaria y redundante, apunta de forma bastante evidente al empleo de los certificados de firma electrónica no basados en dispositivo seguro de creación de firma, muy extendidos.

Concreta el artículo 15.1 de la LAE que:

> "los ciudadanos, además de los sistemas de firma electrónica incorporados al documento nacional de identidad, referidos en el artículo 14, podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos".

Esta previsión es absolutamente redundante con los artículos 13.2.b) y 14 de la LAE, motivo por el que quizá no se encuentra en la LUTICAJ una previsión similar.

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.

Esta diversidad puede implicar un excesivo –e injustificado– esfuerzo técnico y económico por parte de la Administración pública receptora de firmas electrónicas, de forma que la LAE y la LUTICAJ contienen previsiones destinadas a concretar, de todos los sistemas de firma electrónica avanzada potencialmente admisibles, cuáles deben serlo en todo caso; esto es, qué sistemas se benefician de este **derecho de admisión**.

En este sentido, el artículo 21 de la LAE regula, en su apartado 1, criterios para la admisión en general, de forma reglada, mientras que por el contrario, en el apartado 2 regula la admisión de otros sistemas de firma electrónica empleados por las AA. PP., en este caso bajo principios de reconocimiento mutuo y reciprocidad.

El apartado 1 del artículo 21 dispone que:

> "los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por las administraciones públicas como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a disposición de las administraciones públicas la información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas".

Este artículo 21.1 de la LAE establece un marco razonable y equilibrado dentro del cual se puede considerar el derecho de admisión de la firma electrónica. Obviamente, solo los certificados electrónicos reconocidos garantizan una calidad en la identificación del firmante, por lo que no parece haber nada que

objetar en este punto. Asimismo, la condición de **gratuidad en el uso** promueve de forma efectiva la admisión del certificado, que no estaría garantizada en caso de que la Administración debiera pagar un coste al prestador.

Tampoco se puede objetar a la condición de puesta a disposición, por el prestador, de la información que sea precisa, que se refiere a la información sobre el estado de revocación del certificado, si bien genera mayor inseguridad que deban hacerlo "en condiciones que resulten tecnológicamente viables", texto de una cierta oscuridad. En efecto, aunque la LFE no impone un formato técnico ni de certificado ni de mecanismos de información de estado de vigencia de los certificados, todos los prestadores que operan en el mercado se basan en los mismos estándares, por lo que en general se deberá considerar que todos los certificados actualmente emitidos en España son admisibles.

Por su parte, el apartado 2 del artículo 21 de la LAE dispone que:

> "los sistemas de firma electrónica utilizados o admitidos por alguna administración pública distintos de los basados en los certificados a los que se refiere el apartado anterior podrán ser asimismo admitidos por otras administraciones, conforme a principios de reconocimiento mutuo y reciprocidad".

Se trata, por tanto, de una admisión discrecional, a diferencia del caso anterior, que entendemos reglada. Esta distinción se encuentra plenamente justificada, ya que la regla del artículo 21.1 de la LAE regula una relación entre el ciudadano y la Administración que admite su certificado reconocido; mientras que la regla del artículo 21.2 de la LAE regula una relación interadministrativa en la que una Administración admite un documento firmado con un sistema no admisible (por no cumplir las condiciones del artículo 21.1 de la LAE) empleado por otra Administración, lo cual se sujeta –lógicamente– a principios de reconocimiento mutuo y recíproco.

Por lo que respecta a la LUTICAJ, que en este punto se aleja de la LAE, su artículo 22.1 indica que:

> "los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por la Administración de justicia como válidos en las relaciones con la misma, siempre y cuando el prestador de servicios de certificación ponga a disposición de las administraciones competentes en materia de justicia la información que se precise en condiciones que resulten tecnológicamente viables, bajo principios de reconocimiento mutuo y reciprocidad y sin que suponga coste alguno para aquellas".

Los certificados cuya admisión resulta obligatoria deben ser, como en la LAE, certificados reconocidos, tal y como los define y regula la LFE, expedidos por prestadores de servicios de certificación que cumplan sus obligaciones legales; previsión que resulta razonable, dada la ausencia de garantía respecto a la identificación en los certificados no reconocidos.

Asimismo, para que los certificados resulten admitidos, el prestador de servicios que lo emitió debe poner a disposición de la Administración la información que se precise, como en el caso de la LAE, en condiciones que resulten

tecnológicamente viables, texto de una especial oscuridad, que se debe esclarecer acudiendo a los estándares habituales de certificación, como vimos anteriormente.

En definitiva, de todo ello se desprende que el nuevo paradigma legal de certificado de ciudadano a emplear en las relaciones con las administraciones públicas es el denominado certificado en soporte software, como por ejemplo el certificado idCAT emitido por CATCert o el certificado Clase 2 CA emitido por la FNMT-RCM dentro de su proyecto CERES, ampliamente extendidos en ambos casos, siempre dentro de la libre concurrencia que exige la LFE. Esta nueva aproximación no impide, por supuesto, que los ciudadanos, y más en concreto las empresas, decidan adquirir sus propios sistemas de firma electrónica reconocida, algo que resulta muy recomendable, dado que se trata de su clave privada y, por tanto, de su propio riesgo.

CERES

Proyecto CERtificación ESpañola, https://www.cert.fnmt.es/.

4.2.2. La admisión de otros sistemas de firma electrónica

La LAE y la LUTICAJ consideran la posibilidad de admisión de sistemas de firma electrónica avanzada que no se encuentren basados en certificados electrónicos reconocidos, pero dicha previsión no se concreta excesivamente.

El artículo 16.1 de la LAE, que no tiene equivalente en la LUTICAJ, establece que:

> "las administraciones públicas podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, tales como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos".

Aunque habitualmente este artículo se ha empleado para ofrecer soporte normativo a la entrega, por la Administración a los ciudadanos, de sistemas de firma electrónica diferentes de los certificados, también permite a la Administración el empleo de mecanismos de identidad expedidos por terceros, mediante la técnica de la **delegación de la autenticación**.

En este escenario, la Administración admite el uso de sistemas de identificación operados por terceros, incluidos prestadores privados, como Google o Facebook.

Ejemplo

El programa de autenticación electrónica del Gobierno federal de Estados Unidos constituye un buen ejemplo, que hace uso de las identidades provistas, entre otros, por proveedores de servicios de Internet, red social y servicios Cloud para el acceso a determinados procedimientos administrativos, en función del nivel de seguridad y confianza de la credencial. Se trata de una posibilidad prometedora para incrementar la proximidad con el ciudadano, y en casos de uso donde la Administración se relaciona con el mismo a través de los nuevos espacios relacionales de Internet.

4.3. La efectiva admisión de sistemas de firma electrónica

Dos son las notas principales que determinan con carácter general la posibilidad de efectiva admisión, por la Administración, de los diferentes sistemas de firma electrónica:

- El cumplimiento de la LFE por los sistemas a emplear y, en concreto, el empleo de certificados electrónicos que cumplan lo establecido en la LAE y la LUTICAJ.

- La adecuación de los citados sistemas para la función de identificación y garantía de la autenticidad e integridad de los documentos electrónicos; es decir, la determinación de la idoneidad del sistema para el caso concreto.

4.3.1. La verificación del cumplimiento de la legislación de firma electrónica

La primera condición que tanto la LAE como la LUTICAJ establecen en relación con el uso de los sistemas de firma electrónica es que los mismos resulten conforme con la LFE.

Dicha verificación resulta precisa, como resulta fácil de ver, a efectos de confiar en el sistema de firma electrónica a admitir, y corresponde a la Administración actuante realizarla. La verificación del cumplimiento puede resultar bastante compleja, especialmente porque, como ya sabemos, la actividad de prestación de servicios de certificación no se encuentra sujeta a autorización previa y además no se ha dictado ningún reglamento de desarrollo de la LFE que concrete o detalle las condiciones de prestación de dichos servicios.

No hay que olvidar, sin embargo, que los prestadores de servicios de certificación deben comunicar el inicio de su actividad a la autoridad administrativa competente para su supervisión –actualmente la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, del Ministerio de Industria, Energía y Turismo–, de acuerdo con lo que establece el artículo 30 de la LFE, y que dicha información es publicada por el supervisor en su sede electrónica, en forma de base de datos consultable y en forma de lista de servicios de confianza (o TSL) firmada electrónicamente por el citado ministerio.

En el ámbito de la administración electrónica, el uso de los sistemas de firma electrónica se garantiza únicamente, y con carácter general, a aquellos sistemas que cumplan todas las condiciones siguientes:

a) El sistema debe basarse en un certificado reconocido, de uso gratuito para la Administración.

b) El certificado debe haber sido expedido por un prestador que haya comunicado el inicio de su actividad al supervisor y, por tanto, debe aparecer en la TSL correspondiente.

c) El certificado debe cumplir las obligaciones establecidas por el artículo 19 del ENI, como dispone el apartado IV.1 de la Resolución de 19 de julio del 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.

En definitiva, se limita el uso de los sistemas de firma electrónica a los certificados expedidos por prestadores que al menos hayan comunicado al supervisor el inicio de su actividad, asumiendo que en dicho caso los certificados cumplen lo establecido en la LFE, asunción que podría, por supuesto, resultar incorrecta, pues la posibilidad de ser supervisado no equivale a cumplimiento efectivo de la legislación.

Esta opción es la más segura jurídicamente en cuanto a la efectiva admisión, pero no la única, por lo que se debería hacer uso de la potestad discrecional de admisión de otros sistemas de firma electrónica prevista legalmente.

4.3.2. La determinación de la adecuación del sistema de firma electrónica

La segunda condición que establecen la LAE y la LUTICAJ para el uso de un sistema de firma electrónica es que resulte adecuado para garantizar la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

Dicha previsión aparece, a primera vista, como una redundancia en relación con la primera condición, puesto que todos los sistemas de firma electrónica conformes con la LFE deberían ya ser adecuados para la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos. Al menos es lo que dicta la intuición.

Sin embargo, nada más alejado de la realidad: la LFE permite la existencia de sistemas de firma electrónica que muy laxamente identifican a los firmantes. Solo los certificados reconocidos ofrecen realmente una garantía sobre la identidad de los firmantes, y ni siquiera en todos los casos, puesto que la LFE permite la expedición de certificados con seudónimo.

Por tanto, resulta que efectivamente, además de comprobar que el sistema de firma electrónica es conforme con la LFE, se debe evaluar su funcionalidad para determinar si es o no adecuado para su uso en el procedimiento electrónico de que se trate.

La determinación del grado de adecuación de los sistemas de firma electrónica a los procedimientos administrativos electrónicos se realiza a partir de los principios de seguridad mínima y de proporcionalidad. En este caso, la dificultad estriba en disponer de criterios que ayuden en la determinación del nivel de firma electrónica que se requiere en un acto administrativo o del ciudadano.

Una metodología que permita la realización de este análisis de adecuación de uso de un sistema de firma electrónica para una actuación judicial electrónica concreta consideraría los siguientes pasos de evaluación:

- En primer lugar, se debería evaluar la existencia de normativa jurídica que imponga un nivel concreto de firma electrónica a utilizar. Por ejemplo, la legislación impone en algunos casos el uso de la firma electrónica reconocida, con independencia del nivel de riesgo de la operación concreta.

- En segundo lugar, se debería evaluar el derecho del ciudadano o de la Administración a emplear la firma electrónica. Por ejemplo, la normativa de administración electrónica judicial establece el derecho del ciudadano y de los profesionales a emplear el DNI electrónico o determinados sistemas de firma electrónica avanzada o reconocida.

- En tercer lugar, se debería evaluar el nivel de seguridad del activo documental de acuerdo con las dimensiones de seguridad del esquema judicial de interoperabilidad y seguridad, dentro del nivel mínimo marcado por la ley, para determinar necesidades adicionales de seguridad.

- En cuarto lugar, se deberían considerar los requisitos de interoperabilidad del esquema judicial de interoperabilidad y seguridad que resulten aplicables al sistema de firma electrónica en cuestión.

- En quinto y último lugar, se pueden establecer condiciones adicionales en función de cada procedimiento, de acuerdo con lo establecido en el artículo 4 de la LFE.

- Los sistemas de firma electrónica evaluados de esta forma resultarán, en principio, adecuados para la actuación de que se trate.

4.4. El régimen de uso de la firma electrónica

En cuanto al empleo de los sistemas de firma electrónica admitidos, los artículos 12 del RDLAE y 16 de la LUTICAJ establecen dos reglas heterogéneas, agrupadas bajo el epígrafe de régimen de uso de la firma electrónica.

En primer lugar, los artículos 12.1 del RDLAE y 16.1 de la LUTICAJ establecen que el uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación que sean

necesarios de acuerdo con la legislación aplicable. Esta norma recuerda que incluso en el caso de la identificación plena con firma electrónica sigue siendo necesario, al menos potencialmente, el cumplimentado manual de los datos de identidad en el correspondiente formulario o documento administrativo o judicial. Esto es así, ya que en general se admite el uso de la firma electrónica cuando la misma se basa en certificado reconocido, o bien se exige el uso de firma electrónica reconocida.

Se trata de una disposición que inicialmente resulta algo sorprendente, dado que los datos de identificación del firmante ya constan en el certificado electrónico, que además, en la medida que es un certificado reconocido, son datos previamente verificados por el prestador del servicio de certificación.

La comprensión de la norma, sin embargo, se puede encontrar en diversas cuestiones de índole práctica: para empezar, tanto la LAE como la LUTICAJ autorizan el empleo de sistemas de firma electrónica que no se basan en certificados electrónicos, como los basados en contraseñas, en cuyo caso resulta evidente la necesidad de incluir los datos de identidad en el documento; por otra parte, incluso en el caso de uso de firmas electrónicas basadas en certificados, puede suceder que la información de identificación no se encuentre debidamente estructurada, o más correctamente, organizada como se requiere en el formulario, lo cual impide su captura e incorporación automatizadas al documento.

En segundo lugar, los artículos 12.2 del RDLAE y 16.2 de la LUTICAJ establecen que los órganos de la Administración de justicia u organismos públicos vinculados o dependientes podrán tratar los datos personales consignados, a los solos efectos de la verificación de la firma.

En este caso, parece que la finalidad de la regla es aclarar la posibilidad de tratamiento, por sus destinatarios, de los datos personales contenidos o que forman parte del sistema de firma electrónica empleado. De nuevo, aunque inicialmente parece una norma particularmente redundante, lo cierto es que puede evitar dudas innecesarias, especialmente en el caso de los sistemas de firma electrónica que no emplean certificados electrónicos, dada la ausencia de una regulación general que autorice –se entiende que sin solicitar el consentimiento expreso– el uso de los citados datos personales.

4.5. La necesidad de empleo de plataformas de verificación

Los artículos 21.3 de la LAE y 22.2 de la LUTICAJ determinan que las administraciones competentes dispondrán de acceso, al menos, a alguna plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de su competencia, que será de libre acceso por parte de todos los órganos.

Resulta interesante que ya el propio legislador prevea la existencia de servicios de verificación de certificados, sin duda en atención a la complejidad derivada de la verificación de la gran cantidad de certificados emitidos en España en la actualidad, tanto por número de prestadores que operan en territorio español, cuanto por tipos diferentes de certificados expedidos.

Nótese que el texto del artículo resulta un tanto ambiguo, al referirse a la obligación de acceso, "al menos", a "alguna plataforma", indeterminación que remite la decisión a cada administración competente, que deberá aportar el servicio de validación.

Existen actualmente diversas plataformas de verificación de certificados, que ofrecen el servicio de comprobación del estado de vigencia del certificado, así como servicios adicionales, como la extracción semántica de información contenida en los certificados, o incluso validación, completado y preservación de la firma.

En este sentido, cabe recordar que en el ámbito de la administración electrónica, el artículo 25 del RDLAE indica, en su apartado 3, que se creará un sistema nacional de verificación de certificados, formado por plataformas de verificación que podrán delegarse operaciones entre ellas, lo cual incrementa su fiabilidad, y reduce los posibles riesgos en relación con la privacidad.

Asimismo, el RDENI ha regulado, en su artículo 20, el conjunto mínimo de requisitos aplicables a las plataformas de validación de certificados y firmas electrónicas, en los siguientes términos:

- De acuerdo con el apartado 1 del artículo 20 del RDENI, el objeto de las plataformas de validación de certificados electrónicos y de firma electrónica es proporcionar servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, lo cual incluye servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las administraciones públicas.

- El apartado 2 del mismo artículo 20 del RDENI ordena que dichos sistemas proporcionen, en un único punto de llamada, todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios para integrar los distintos certificados reconocidos y firmas que pueden encontrase en los dominios de dos administraciones diferentes, lo cual realmente se puede considerar como una verdadera norma de interoperabilidad.

- Por su parte, el apartado 3 del artículo 20 del RDENI indica que dichos sistemas deberán potenciar la armonización técnica y la utilización común de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como

el análisis de los campos y extracción univoca de la información pertinente; norma que parece más dirigida a establecer una función de normalización que de interoperabilidad, en sentido estricto, y que sin la necesaria base legal difícilmente resultará operativa.

- Finalmente, el apartado 4 del artículo 20 del RDENI establece que las plataformas en cuestión incorporarán las listas de confianza de los certificados interoperables entre las distintas administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza (TSL).

5. Las estrategias de conservación a largo plazo de documentos firmados

Se pueden establecer diversas estrategias de conservación a largo plazo de los documentos firmados.

En primer lugar, mientras el documento electrónico de archivo firmado se encuentra en fase activa o de tramitación, se pueden aplicar las siguientes estrategias:

- Adición de sellos de fecha y hora de archivo (*ArchiveTimeStamp*) a cada objeto de firma electrónica. Este método resulta adecuado para proteger cada firma y los datos que contiene, pero no protege otras informaciones complementarias de la firma ni los metadatos correspondientes, que se encuentran fuera del objeto de firma y pueden tener relevancia probatoria en caso de conflicto.

- Adición de sellos de fecha y hora a cada instancia descriptiva de firma electrónica. Este método resulta adecuado para proteger la firma unitaria y las informaciones complementarias y los metadatos correspondientes, especialmente en caso de uso de un repositorio seguro.

- Adición de sellos de fecha y hora a cada secuencia de firma electrónica. Este método resulta adecuado para proteger todas las firmas de un flujo y las informaciones complementarias y los metadatos correspondientes, también en el escenario de repositorio seguro.

En segundo lugar, mientras el documento electrónico de archivo firmado se encuentra en fase semiactiva o de vigencia, se pueden aplicar las estrategias adicionales:

- Adición de sellos de fecha y hora de archivo (*ArchiveTimeStamp*) a la foliación de un expediente electrónico. En lugar de añadir un nuevo sello de archivo a cada firma de cada documento, solo se añade un sello en la firma de la foliación, ya que este elemento protege todos los documentos del expediente, lo que representa una vía computacional más eficiente de protección de la firma que la protección individual de cada objeto de firma.

- Empaquetado de los documentos del expediente, incluyendo la foliación, en un contenedor firmado, y adición de sellos de fecha y hora de archivo (*-) a la firma del contenedor. Se podría emplear para proteger paquetes de expedientes enteros, por ejemplo por años, lo cual siempre es más eficiente que resellar cada expediente.

Finalmente, si el documento electrónico de archivo firmado pasa a fase de conservación permanente, hay que recordar que en todo caso el documento electrónico ha perdido ya su valor legal y, por tanto, en general se puede defender la no necesidad de preservar ni mantener la evidencia de todas las informaciones que soportan las firmas electrónicas, sin perjuicio de aplicar técnicas de seguridad para garantizar la autenticidad de los contenidos de los repositorios digitales de archivo, eminentemente mediante metadatos y pistas de auditoría.

Actividades

1. Identificad casos de uso de firma electrónica en el sector privado y en el procedimiento administrativo electrónico.

2. Preparad una estrategia de autenticación de documentos, y de conservación de los mismos.

Bibliografía

Alamillo Domingo, I. (2012). "Seguridad y firma electrónica: marco jurídico general". En: E. Gamero Casado; J. Valero Torrijos (coords.). *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Aranzadi Thompson Reuters, Cizur Menor.

Alamillo Domingo, I.; Urios Aparisi, X. (2004). "Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica". *Revista de la Contratación Electrónica* (núm. 46).

Alamillo Domingo, I.; Urios Aparisi, X. (2010). "El nuevo régimen legal de gestión de la identidad y firma electrónica por las Administraciones Públicas". En: L. Cotino Hueso; J. Valero Torrijos (coords.). *Administración electrónica: la Ley/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*. Valencia: Tirant lo Blanch.

Linares Gil, M. (2010). "Identificación y autenticación de las Administraciones Públicas". En: E. Gamero Casado; J. Valero Torrijos (coords.). *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*. Aranzadi Thompson Reuters, Cizur Menor.

Linares Gil, M. (2012). "Identificación electrónica de los órganos judiciales y autenticación del ejercicio de su competencia". En: E. Gamero Casado; J. Valero Torrijos (coords.). *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Aranzadi Thompson Reuters, Cizur Menor.

Martín Delgado, I. (2010). "Identificación y autenticación de los ciudadanos". En: E. Gamero Casado; J. Valero Torrijos (coords.). *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*. Aranzadi Thompson Reuters, Cizur Menor.

Martín Delgado, I. (2012). "Identificación electrónica de ciudadanos y profesionales en el ámbito de la justicia". En: E. Gamero Casado; J. Valero Torrijos (coords.). *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Aranzadi Thompson Reuters, Cizur Menor.

Martínez Gutiérrez, R. (2011). "Identificación y autenticación: DNI electrónico y firma electrónica". En: J. L. Piñar Mañas (dir.). *Administración electrónica y ciudadanos*. Civitas Thompson Reuters, Cizur Menor.

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

Martínez Nadal, A. (2004). *Comentarios a la Ley 59/2003 de firma electrónica*. Madrid: Civitas.

Martínez Nadal, A. (2006). "Firma electrónica, certificados y entidades de certificación". *Revista de Contratación Electrónica* (núm. 68).

Ortega Díaz, J.F. (2008). *La firma y el contrato de certificación electrónicos*. Aranzadi, Cizur Menor.

Pérez Pereira, M. (2009). *Firma electrónica: contratos y responsabilidad civil*. Aranzadi, Cizur Menor.