View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Diposit Digital de Documents de la UAB

TRABAJO DESARROLLADO PARA LA OBTENCIÓN DE LA SUFICIENCIA INVESTIGADORA EN EL PROGRAMA DE DOCTORADO EN SEGURIDAD Y PREVENCIÓN

Las políticas de firma electrónica en la Administración electrónica

Por:

Ignacio Alamillo Domingo

Dirigido por el Dr. Ramón-Jordi Moles i Plaza
Profesor Titular de Derecho Administrativo de la Universitat Autònoma de Barcelona

Septiembre de 2012

ÍNDICE

1 INTRODUCCIÓN GENERAL

En este trabajo abordamos el estudio de la Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración, atendiendo a su concepto y finalidades, contenidos y semántica, y efectos jurídicos, principalmente en el ámbito de la Administración electrónica[1].

Antes, sin embargo, procede realizar un breve repaso a las políticas de autenticación y firma electrónica en la Administración electrónica, así como presentar muy brevemente el marco regulatorio correspondiente y, en concreto, el encuadramiento de la Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración.

1.1 UNA VISTA RÁPIDA A LAS ACTUALES POLÍTICAS DE AUTENTICACIÓN Y FIRMA EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA

1.1.1 La firma electrónica ha sido, y seguirá siendo, un elemento clave en el desarrollo de la Administración electrónica

Las Administraciones Públicas españolas han realizado un esfuerzo importante en los últimos años para garantizar a los ciudadanos su derecho a relacionarse electrónicamente con las Administraciones, un impulso que ha permitido, en opinión del Ministerio de Hacienda y Administraciones Públicas, "alcanzar una posición de liderazgo en el desarrollo de la Administración Electrónica, de modo que los resultados de 2010 del informe "eReadiness" de la Organización de las Naciones Unidas sitúan a España en el noveno puesto del ranking mundial (el quinto en el subindicador

[1] Sin perjuicio del reconocimiento del valor e interés de este instrumento en otros sectores, como el comercio electrónico privado, donde resulta perfectamente aplicable, aunque con diferencias principalmente referidas a la semántica de la firma electrónica.

específico de servicios electrónicos on-line) y en el quinto del europeo[2]".

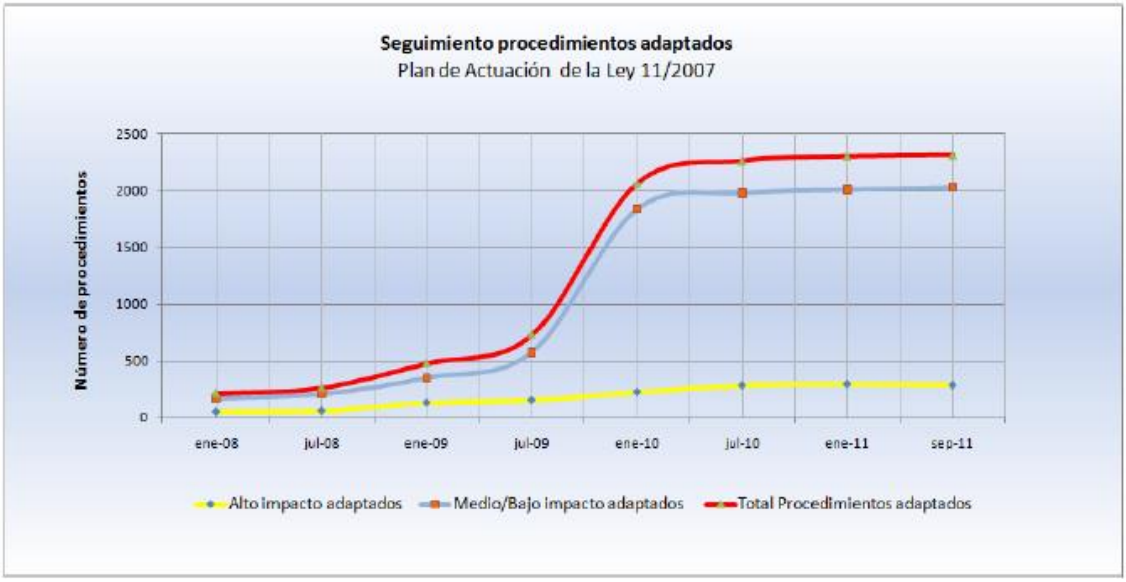
La firma electrónica resulta una pieza esencial en el funcionamiento de la Administración electrónica. Como ha puesto de manifiesto PIÑAR MAÑAS, 2011: pp. 51 y 52, "la desvinculación territorial que deriva de la implantación de nuevas tecnologías y la posibilidad de configurar relaciones jurídicas no presenciales requiere implantar mecanismos que garanticen la seguridad del sistema y que acrediten, al menos, la identidad de los sujetos, el contenido de las declaraciones de voluntad o de los documentos y la acreditación de su emisión y recepción", recordando que, de acuerdo con la Comunicación de la Comisión Europea COM (2003) 567, la autenticación y la gestión de identidad constituyen temas principales, siendo imprescindible poder garantizar una identidad cierta y única de cada persona, mediante la firma electrónica.

En efecto, la firma electrónica se ha desarrollado de forma muy importante en el sector público, en particular en el procedimiento administrativo electrónico, tanto en España como en la Unión Europea, y se puede decir que, lejos de decaer, la institución goza de buena salud.

Y es que, en la actualidad, en el ámbito de la Administración General del Estado se han adaptado ya a la legislación de administración electrónica más de 2.300 procedimientos y servicios electrónicos, lo que supone que, aproximadamente, un 90% de sus procedimientos y un 99 % de la tramitación total anual pueden realizarse ya por medios electrónicos, como se puede apreciar en el siguiente gráfico[3]:

[2] Informe de la Secretaría de Estado para la Función Pública, presentado al Consejo de Ministros el 16 de septiembre de 2011, sobre la situación de la administración electrónica en la Administración General del Estado.

[3] Íbidem.



Por su parte, también las Administraciones de las Comunidades Autónomas han ido incorporando de forma progresiva la tramitación electrónica, como se aprecia en el siguiente gráfico, referido al año 2010:

Tabla 10. Inventario de Procedimientos 2010

CC.AA.	N° Procedimientos Inventariados	N° Procedimientos Inicio Electrónico	Proced. Electrónicos/ Proced. Inventariados (%)
Andalucía	1.230	1.018	83%
Aragón	1.100	200	18%
Principado de Asturias	ND	ND	ND
Illes Balears	664	53	8%
Canarias	1.355	19	1%
Cantabria	794	794	100%
Castilla-La Mancha	1.341	692	52%
Castilla y León	1.180	398	34%
Cataluña	1.611	303	19%
Comunitat Valenciana	2.062	508	25%
Extremadura	1.198	69	6%
Galicia	1.917	152	8%
Comunidad de Madrid	876	860	98%
Región de Murcia	1.173	60	5%
Navarra	2.027	2.027	100%
País Vasco	671	176	26%
La Rioja	749	433	58%
Ceuta	200	200	100%
Melilla	ND	ND	ND
Total	**20.148**	**7.962**	**40%**

Asimismo, el número de verificaciones de firmas electrónicas resulta un indicador significativo para evaluar el nivel de uso efectivo de este instrumento. En este sentido, la plataforma @firma realizó 66.808.740 operaciones de verificación de firma sólo en 2011[4].

También la reciente Propuesta de Agenda Digital para España, presentada por los Ministerios de Industria, Energía y Turismo, y de Hacienda y Administraciones Públicas el 25 de julio de 2012 atiende a la necesidad de potenciar la Administración electrónica.

Como indica el texto, "uno de los grandes retos a los que se enfrenta la Administración Pública en los próximos años es el de incrementar la productividad de nuestras Administraciones para conseguir una reducción del gasto público, manteniendo al mismo tiempo unos servicios públicos universales y de calidad. Para ello es imprescindible conseguir un sector público capaz de proporcionar servicios de alto valor añadido, adaptados a las necesidades de ciudadanos y empresas, que aporten un valor claro y definido a quienes los utilizan, y que hagan un uso inteligente de los recursos disponibles. Además, todo ello habrá que conseguirlo en un entorno de austeridad presupuestaria. La administración electrónica, o e-Administración, es uno de los pilares esenciales para hacer frente a estos retos, ya que su utilización ahorra costes innecesarios tanto para los ciudadanos y empresas, como para la propia Administración; contribuye a optimizar los procesos administrativos y a acercar la Administración a los ciudadanos", toda una declaración de intenciones que se complementa con medidas concretas referidas a la autenticación y la firma electrónica:

- Objetivo 3.1. Avanzar hacia una Administración integrada en la sociedad con servicios públicos de calidad centrados en ciudadanos y empresas:
    - 2. Avanzar en la creación de servicios transfronterizos en el seno de la Unión Europea para facilitar la movilidad de ciudadanos y empresas así

[4] Cfr. Boletín de indicadores de Administración electrónica de junio de 2012, del Observatorio de Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas.

como la identificación digital europea.

- Objetivo 3.2. Incrementar el uso de los servicios públicos electrónicos por parte de ciudadanos y empresas:
    - 1. Facilitar los mecanismos de identificación y autenticación frente a la Administración mediante:
        - La potenciación los sistemas de identificación y firma electrónica en los servicios públicos electrónicos.
        - El desarrollo de soluciones de movilidad que faciliten la identificación mediante el uso de dispositivos móviles.
        - La traslación de mejores prácticas del sector privado al ámbito de la identificación en los servicios públicos electrónicos.
- Objetivo 3.3. Racionalizar y optimizar el empleo de las TIC en las Administraciones Públicas:
    - 2. Desarrollar estrategias que permitan optimizar los recursos disponibles:
        - Avance hacia una administración sin papeles de forma que se automaticen todos los procedimientos y procesos administrativos, y se aumente el conocimiento y habilidades de los empleados públicos mediante tecnologías de trabajo colaborativo, sistemas de identificación y firma electrónica, y servicios de Administración Electrónica.
- Objetivo 3.5. Emplear la tecnología para proporcionar mejores servicios públicos:
    - 5. Empleo del DNIe como mecanismo de identificación de usuarios alternativo a la Tarjeta Sanitaria.
    - 6. Acceso en línea de los ciudadanos a su historia clínica digital desde

cualquier punto por medio del DNIe.

- Objetivo 4.1. Impulsar el mercado de los servicios de confianza:
    - 2. Impulsar el desarrollo y uso de servicios de identidad y firma electrónicas adecuados para las distintas necesidades de los usuarios y prestadores.
    - 3. Reforzar el DNIe como instrumento de identidad electrónica general favoreciendo su uso intensivo y el aprovechamiento de sus ventajas en el contexto digital adecuado.
    - 4. Refuerzo de la capacidad supervisora de la Administración, impulsando procesos de auditoría y certificación y asegurando su armonización y el reconocimiento mutuo con las iniciativas europeas.

Como se puede constatar, nos encontramos ante una materia de prometedor futuro, al menos en el ámbito de la Administración electrónica… en especial si la legislación y la reglamentación que la desarrolle cumplen con los necesarios parámetros de calidad y seguridad jurídica.

1.1.2 La interoperabilidad en la firma electrónica forma parte de la agenda política de la Unión Europea, en particular, para las operaciones transfronterizas

La firma electrónica, a pesar de haber sido objeto de una cierta armonización por la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la firma electrónica (DO L 13, de 19/01/2000, en adelante, la "DFE"), plantea muchos problemas en las operaciones transfronterizas.

La Agenda Digital para Europa aprobada por la Comisión Europea incluye diversas medidas de impulso de la firma electrónica en el ámbito de los servicios

transfronterizos dentro de la Unión Europea, muestra del interés práctico de la figura y, a la vez, de los retos pendientes, incluyendo medidas legales en relación con la firma electrónica (acción clave nº 3) y el reconocimiento mutuo de la identificación y la autenticación electrónicas (acción clave nº 16)[5].

También se debe reseñar que el Acta del Mercado Único propuesta por la Comisión Europea ha previsto, entre sus doce prioridades, la de avanzar hacia un mercado único digital, para lo cual considera, como primera medida, disponer de una "legislación que garantice el reconocimiento mutuo de la identificación y autentificación electrónicas en toda la UE y revisión de la Directiva sobre la firma electrónica. El objetivo es conseguir una interacción electrónica segura y sin obstáculos entre empresas, ciudadanos y administraciones públicas para aumentar, incluso en su dimensión transfronteriza, la eficacia de los servicios, de los contratos públicos, de la prestación de servicios y del comercio electrónico", para la cual se "propondrá un nuevo marco legislativo para garantizar la confianza en las transacciones electrónicas. Dicho marco incluirá la revisión de la Directiva sobre la firma electrónica con objeto de aclarar sus conceptos, simplificar el uso de la firma y eliminar los obstáculos a la interoperabilidad. El marco garantizará también el reconocimiento mutuo de los servicios de identificación y de autentificación electrónicas y abordará el funcionamiento transfronterizo de algunos otros servicios de confianza"[6].

Y casi causa sorpresa la referencia explícita que la Comisión Europea realiza, en su Hoja de ruta para la estabilidad y el crecimiento[7], a la necesidad de "ofrecer una base jurídica común para el reconocimiento mutuo de la autenticación y la firma electrónicas más allá de las fronteras nacionales", que sitúa entre las medidas cuya aplicación pueden dar un impulso al crecimiento y el empleo a la escala de la Unión Europea.

Por todo ello, se comprende perfectamente la reciente publicación de una Propuesta

[5] COM (2010) 245 final/2: pp. 14 y 38.

[6] COM (2011) 206 final: p. 14.

[7] COM (2011) 669 final: p. 7.

de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior[8], con el objeto de "hacer posibles unas interacciones electrónicas seguras y sin fisuras entre empresas, ciudadanos y autoridades públicas con el fin de aumentar la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la UE", y un interesante cambio de enfoque sobre la materia regulada.

En dicho documento se constata que "no existe ningún marco transfronterizo e intersectorial global de la UE para garantizar la seguridad, fiabilidad y sencillez de las transacciones electrónicas que incluya la identificación, la autenticación y la firma electrónicas", y por tanto, se establece como objetivo "mejorar la legislación existente y ampliarla incluyendo el reconocimiento y la aceptación mutuos a nivel de la UE de los sistemas de identificación electrónica notificados y otros servicios de confianza electrónicos conexos esenciales".

La propuesta se justifica, junto a la falta de confianza por los ciudadanos europeos, indicando que "las divergencias en la aplicación en cada país de la Directiva sobre la firma electrónica, debidas a diferente interpretación por parte de los Estados miembros, han creado problemas de interoperabilidad transfronteriza y, por ende, segmentado la situación en la UE y distorsionado el mercado interior"[9].

Asimismo, continúa diciendo la Comisión, para justificar el valor añadido de la intervención de la Unión Europea, que "la acción a nivel de la UE produciría unos beneficios indudables en comparación con la acción a nivel de los Estados miembros. La experiencia ha demostrado ciertamente que las medidas nacionales no solo resultan insuficientes para hacer posibles las transacciones electrónicas a través de las fronteras, sino que, por el contrario, han creado obstáculos a la interoperabilidad de las firmas electrónicas en la UE y están teniendo actualmente el mismo efecto en relación con la identificación y la autenticación electrónicas y los servicios de confianza

[8] COM (2012) 238 final.

[9] Cfr. COM (2012) 238 final: pp. 50 y 51.

conexos"[10].

Finalmente, la Comisión considera que "la propuesta de Reglamento aportará un marco jurídico favorable a la amplia adopción de los proyectos piloto a gran escala que se han puesto en marcha a nivel de la UE para apoyar el desarrollo de medios de comunicación electrónica interoperables y fiables (entre ellos SPOCS, que respalda la aplicación de la Directiva sobre los servicios; STORK, que apoya el desarrollo y la utilización de identificaciones electrónicas interoperables; PEPPOL, que apoya el desarrollo y la utilización de soluciones de contratación electrónica interoperables; epSOS, que apoya el desarrollo y la utilización de soluciones de sanidad electrónica interoperables; y eCodex, que apoya el desarrollo y la utilización de soluciones de justicia electrónica interoperables)"[11].

1.2 EL FRAGMENTARIO MARCO REGULATORIO ESPAÑOL DE LA POLÍTICA DE FIRMA ELECTRÓNICA Y CERTIFICADOS EN LA ADMINISTRACIÓN ELECTRÓNICA

La política de firma electrónica y de certificados de la Administración se regula, de forma fragmentaria mediante un variado conjunto de normas que, como si de retales se tratase, caracterizan la institución de forma parcial, incompleta e inconsistente.

En efecto, en primer lugar podemos mencionar, el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica (BOE núm. 25 de 29/01/2010, en adelante, el "RDENI") trata, dentro del concepto de interoperabilidad[12], de la firma electrónica y los

[10] Ibídem.

[11] Ibídem: p. 51.

[12] La interoperabilidad se define, en el anexo de la LAE, apartado o), como "la capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos". Para un análisis del que ha denominado "carácter poliédrico de la interoperabilidad" y la regulación española, cfr. CERRILLO I MARTÍNEZ, 2010: pp. 784 y ss.

certificados, en su capítulo IX, artículos 18 a 20, con un especial protagonismo a la denominada "política de firma electrónica y de certificados".

Dichos artículos suponen un desarrollo clave del régimen de uso de la firma electrónica en el procedimiento administrativo electrónico, puesto que condicionan, para todas las Administraciones Públicas y de forma absolutamente esencial, el uso de este instrumento de identificación y autenticación, regulado en el capítulo II del Título segundo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (BOE núm. 150 de 23/06/2007, en adelante, la "LAE"), dentro del marco general de uso de la firma electrónica previsto en la Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE núm. 304 de 20/12/2003, en adelante, la "LFE").

En segundo lugar, y también con carácter general, prevé el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (BOE núm. 25 de 30/01/2010, en adelante, el "RDENS") diversas reglas sobre firma electrónica, sustancialmente en su artículo 33 y epígrafe 5.7.4 del anexo II que le acompaña.

Y en el ámbito de la Administración General del Estado, en tercer lugar, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (BOE núm. 278 de 18/11/2009, en adelante, "RDLAE"), ya había establecido, entre las disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad, su propia regulación de la política de firma electrónica y de certificados, referida a los "requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y sus organismos públicos", lo que da cumplida cuenta de la importancia de este instrumento, y de los riesgos derivas de los excesos regulatorios.

Además, en cuarto lugar, debemos mencionar la existencia de diversas Normas Técnicas de Interoperabilidad, dictadas en desarrollo del RDENI, que se refieren a la firma electrónica, en particular:

- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función

Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico (BOE núm. 182, de 30/07/2011).

- Resolución de 19 de julio de 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 (BOE núm. 182, de 30/07/2011).

Finalmente, el desarrollo previsto[13] 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 (BOE núm. 160 de 06/07/2011, en adelante, la "LUTICAJ") considera la existencia de una política de firma electrónica y de certificados para su utilización en dicho ámbito por parte de los ciudadanos, los profesionales y los órganos de la Administración de Justicia u organismos públicos vinculados o dependientes[14].

Y por lo que se refiere al ámbito de la Unión Europea, también las políticas de firma electrónica resultan relevantes, en tanto en cuanto, como veremos, se conforman como uno de los elementos que permiten el despliegue de servicios públicos electrónicos transfronterizos, en particular de forma conjunta con la nueva reglamentación propuesta de identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior, a la que nos hemos referido anteriormente.

En este sentido, conviene citar ya en este lugar las dos importantes Decisiones de la Comisión Europea reguladoras del uso transfronterizo de la firma electrónica:

- La Decisión de la Comisión 209/767/CE, de 16 de octubre de 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

[13] Se puede acceder a las Guías técnicas de interoperabilidad y seguridad judicial del Consejo General del Poder Judicial para ver el tratamiento propuesto para la firma de los documentos judiciales, publicadas en el Test de Compatibilidad del Punto Neutro Judicial http://testcompatibilidad.pnj.cgpj.es/cgpjtest/php/main.php (último acceso: 23/06/2012).

[14] Dicha política de firma electrónica aún no ha sido objeto de aprobación, por lo que en este trabajo no

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 de 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 Decisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE, relativa a los servicios en el mercado interior.

1.3 ALGUNOS CONCEPTOS PREVIOS SOBRE EL RÉGIMEN JURÍDICO GENERAL DE LA FIRMA ELECTRÓNICA

Antes de abordar el estudio detallado de la política de firma electrónica, resulta obviamente necesario analizar con cierto detalle el objeto que regula la citada política, que no es otro que el uso de la firma electrónica en el ámbito de la Administración electrónica, lo cual conlleva, de forma ineludible, el análisis de la regulación general en esta materia.

La Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE núm. 304 de 20/12/2003, en adelante, la "LFE"), dictada en cumplimiento de la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la firma electrónica (DO L 13, de 19/01/2000, en adelante, la "DFE"), regula la firma electrónica, y los elementos que le ofrecen soporte, con carácter horizontal al ordenamiento jurídico español[15], definiendo la firma electrónica y 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

abordamos su análisis detallado.

[15] Lo cual no ha sido suficiente para evitar la creación de todo un marco regulatorio sectorial en el ámbito de la Administración electrónica.

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[16].

Podemos avanzar que la firma electrónica es un concepto funcional, supuestamente neutral desde la perspectiva tecnológica; es decir, se trata de una descripción de funciones que muchas tecnologías pueden realizar[17]. 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 las dichas 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

[16] No constituye objeto del presente trabajo entrar en los detalles del estatuto de funcionamiento de los prestadores de servicios de certificación – por otra parte muy ampliamente analizado por la doctrina mercantil de nuestro país – sin perjuicio de la realización de alguna referencia puntual derivada del análisis del uso de los certificados en la normativa de Administración electrónica.

[17] ILLESCAS ORTIZ, 2001: p. 53 ha criticado que la DFE y, por consiguiente, la legislación española (en referencia al RDL 14/99) no adopte un tratamiento plenamente neutral sobre la firma electrónica, sino dualista o bifronte, decantándose por establecer una disciplina privilegiada para la tecnología de firma electrónica más difundida en la práctica contemporánea del comercio electrónico; esto es , para las firmas basadas en la existencia de una doble clave – pública y privada – y en la intervención de un denominado prestador de servicios de certificación.

que se puede emplear directamente[18].

- Es necesario interpretar los requisitos de integridad y autenticidad documental (así como el incorrectamente denominado "no repudio"[19]) 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[20]. 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.

- 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 sólo unos pocos artículos de la LFE:

---

[18] A pesar de lo cual resulta llamativo que las nuevas legislaciones expliciten el uso de la firma electrónica, algo que frecuentemente causa más problemas de interpretación que clarifica la cuestión. En efecto, cuando algunas leyes se refieren a que un trámite o acto se puede autorizar con firma escrita o electrónica indistintamente, mientras que otras leyes no incluyen – por innecesaria – esta referencia doble, algunos operadores jurídicos interpretan que en este segundo caso el legislador no ha querido que se pueda emplear la firma electrónica, conclusión a nuestro juicio claramente incorrecta desde un punto de vista lógico.

[19] En nuestra opinión, se debería ir abandonando esta denominación, préstamo del inglés "non repudiation", en beneficio de la más correcta de "no refutación", entre otros motivos, porque lo que la firma electrónica persigue es evitar una falsa refutación por el firmante de la imputación de la autoría del documento (mientras que el término legal de "repudio" se ha empleado tradicionalmente en Derecho español para el repudio de la esposa por el marido). En este sentido, además, la normativa técnica principalmente aplicable ha sido modificada en el sentido de sustituir este concepto ("non repudiation") por el de compromiso con el contenido ("content commitment").

[20] De esta forma se plasma, como veremos, en el artículo 4 de la LFE. Cfr. la sección 1.4 de este trabajo.

- El artículo 3, sin duda el más importante, por cuanto define la firma electrónica, el documento electrónico y establece su validez y efectos jurídicos; y que hay que 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 que los intermediarios de la firma electrónica no serán responsables jurídicamente, y en concreto, el apartado 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; regulación que sólo muy tangencialmente abordamos en este trabajo y sobre la cual nos remitimos a la notable

bibliografía existente en nuestro país[21].

1.3.1 Los diferentes "tipos" de firma electrónica

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

Como se indica en la Agenda Digital para Europea[22], "las tecnologías de identidad electrónica (eID) y los servicios de autenticación resultan esenciales para las transacciones en internet, tanto en el sector público como en el privado. Actualmente, la forma más habitual de autenticar es utilizar contraseñas. Esto puede resultar suficiente para muchas aplicaciones, pero va aumentando la necesidad de soluciones más seguras", texto que recuerda la existencia de múltiples niveles de firma y la necesidad de tener presente métodos para determinar su adecuación a cada caso concreto.

1.3.2 La simple 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".

---

[21] Entre otros, podemos citar a MARTÍNEZ NADAL, 1998 y 2004; ÁLVAREZ-CIENFUEGOS SUÁREZ, 2000; ILLESCAS ORTIZ, 2001; GARCÍA MAS, 2002; ORTEGA DÍAZ, 2008; y PÉREZ PEREIRA, 2009.

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 privadas, 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.

1.3.3 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 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").

En este sentido, ELÍAS BATURONES, 2008: p. 49, ha señalado, precisamente, las diferencias con a la firma manuscrita, indicando que "la cuestión es que, en una firma tradicional, aparece el nombre y apellidos de su autor junto con la rúbrica, que sirve de impronta a la hora de vincular a la persona que firma el documento con su contenido, mientras que, en la firma electrónica, se acentúa más la identidad entre el autor con el contenido, resumiendo una parte esencial del mismo, cifrándolo posteriormente, con la fecha y hora de la emisión, por lo que la menor variación del algoritmo, así obtenido,

[22] COM (2010) 245 final/2, p. 13.

supondría una prueba de manipulación externa que derivaría a la existencia de un tercero no querido, y posiblemente malintencionado, entre las partes en cuestión".

La definición se corresponde con las funciones tradicionales de la firma manuscrita, de modo que la firma avanzada resulta idónea ya 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, que tendremos ocasión de exponer detalladamente[23].

Base ahora 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, como veremos inmediatamente, reconocida).

1.3.4 La firma electrónica reconocida

Contiene, finalmente, la LFE una tercera definición de firma electrónica, en su artículo 3.3, en virtud del 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 cualifica especialmente como equivalente a la firma manuscrita[24], y sin que ello implique la discriminación de los restante 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

[23] Cfr. sección 5.1.2 de este trabajo.

[24] VALERO TORRIJOS, 2007: p. 42, considera llamativa la continua referencia que se realiza en la LAE a la firma electrónica avanzada, y no a la reconocida, a la cual considera como "la única que tiene garantizada legalmente y de forma automática la equivalencia con la firma manuscrita desde el punto de vista de la eficacia".

profesional usuario de servicios privados y públicos, se identifique y firme.

1.3.5 La eficacia y prueba 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 sirva al objetivo de imputar el contenido del documento a la persona que lo autoriza.

Esto es, 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, y 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 en 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 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.

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, determina el artículo 3.4 de la LFE 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, como ya hemos visto, 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, en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica; esto es, que toda firma – como hemos avanzado anteriormente – 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.

Es precisamente esta prueba de la autenticidad de la firma electrónica la que se debe 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 se puede reconducir a la unidad.

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, que en su caso podrá simplificarse mediante la aportación, por los prestadores de los servicios de seguridad o de los servicios de certificación de la firma electrónica, o por lo fabricantes de la tecnología, de certificados que acrediten, conforme a la normativa industrial o conforme a un esquema nacional de evaluación y acreditación de la seguridad de las tecnologías de la información, que los servicios y los productos empleados cumplen los requisitos de seguridad aplicables al caso concreto.

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), mientras que 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 restante 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.

1.4 LA REGULACIÓN INICIAL DE LAS CONDICIONES ADICIONALES AL USO DE LA FIRMA ELECTRÓNICA EN EL PROCEDIMIENTO

La LFE dispone, en su artículo 4, determinadas especialidades en el uso de la firma electrónica en la Administración, conocidas en la DFE de forma genérica como "la excepción del sector público".

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 aquéllas y éstos 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 8ª, 18ª, 21ª y 29ª, y que hoy ha sido complementada y ampliada de forma importante por la LAE y la LUTICAJ[25].

Es cierto, sin embargo, que la LFE no determina su ámbito subjetivo de aplicación más

[25] Como veremos posteriormente, hay que hacer notar el carácter de leyes especiales de la LAE y la LUTICAJ con respecto a la LFE.

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.

Veremos, por tanto, la caracterización legal de las condiciones adicionales y los mecanismos para la verificación de su cumplimiento, cuando se establezcan.

1.4.1 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[26], 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 sólo podrán hacer

[26] Esta posibilidad se contiene en el artículo 3.7 de la DFE, y se conoce como la "excepción del sector público".

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", por cuanto 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, 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", siguiendo a la DFE fielmente. 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[27].

En efecto, como tendremos ocasión de verificar *infra*, algunas de las condiciones adicionales exigidas en el ámbito de la administración electrónica[28] impiden de plano el empleo de certificados expedidos por prestadores de Estados miembros de la Unión Europea, en posible infracción del artículo 4 de la LFE y el artículo 3.7 de la DFE, del que trae causa.

---

[27] DUMORTIER *et al*., 2003: pp. 40 y ss., p. 99. y p. 148 y ss., han advertido sobre las dificultades de interpretación de algunos de los requisitos del artículo 3.7 de la DFE, como la necesidad de que las condiciones adicionales se refieran sólo a las características específicas de la aplicación de que se trate. Asimismo, indican que el establecimiento de condiciones generales de carácter general para todas las aplicaciones de administración electrónica pueden afectar seriamente a la libre competencia del mercado de servicios y productos de firma electrónica, en cuyo caso la Comisión Europea debería intervenir, de acuerdo con lo establecido en la DFE y en el artículo 86 del Tratado de la Comunidad Europea. En concreto, dichos autores explicitan el riesgo de que las agencias públicas restrinjan sus aplicaciones a determinados certificados nacionales, en clara infracción del art. 3.7 de la DFE (como ha venido sucediendo en España hasta la LAE. En el ámbito de las relaciones con la AEAT, hasta la Orden HAC/1181/2003, de 12 de mayo, únicamente se podía emplear el certificado Clase 2 CA de la FNMT-RCM).

[28] Por ejemplo, la exigencia de inclusión dentro del certificado de un extranjero del NIF español que tiene asignado – impuesta en aplicación de la Orden HAC/1181/2003, de 12 de mayo – impide de forma práctica que dicho extranjero pueda emplear su sistema nacional de firma electrónica para realizar

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 de la Comisión 209/767/CE, de 16 de octubre de 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 de 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 Decisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE, relativa a los servicios en el mercado interior.

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[29].

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

---

trámites con la AEAT.

[29] Nótese que la Decisión 2011/130/UE se refiere a documentos producidos por las Autoridades competentes, que deben ser admitidos por las restantes Autoridades en la Unión Europea, mientras que la Decisión 2009/767/CE tiene un alcance más genérico, aplicable también a otros documentos que presentan los ciudadanos a las Autoridades competentes.

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[30].

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 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[31] y de Industria, Turismo y Comercio[32], 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, que veremos posteriormente[33].

Nada se dice acerca de la aprobación de condiciones adicionales, generales o particulares, por parte de otras Administraciones públicas, ni tampoco respecto de la

[30] Cosa diferente sería la extensión obligatoria e indiscriminada de dichas condiciones adicionales al sector público, que podría suponer restricciones a la libre competencia incompatibles con el derecho europeo.

[31] Esta competencia, en la actualidad, correspondería al Ministerio de Hacienda y Administraciones Públicas.

[32] Esta competencia, en la actualidad, correspondería al Ministerio de Industria, Energía y Turismo.

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 hemos visto sucede en el caso de la Directiva de servicios; y que el instrumento normativo apropiado sería el reglamento[34], 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.

En cualquier caso, debe considerarse como una condición adicional general, aplicable a los prestadores cuyos certificados se admitan ante la Administración General del Estado, la prevista en el artículo 23.2 del RDLAE, que dispone que "los prestadores de servicios de certificación deberán facilitar a las plataformas públicas de validación que se establezcan conforme a lo previsto en este real decreto, acceso electrónico y gratuito para la verificación de la vigencia de los certificados asociados a sistemas utilizados por los ciudadanos, la Administración General del Estado y sus organismos públicos", en línea con lo establecido en el artículo 21.1 de la LAE.

Asimismo, son condiciones adicionales generales, en este caso, aplicables a los prestadores cuyos certificados se admitan ante cualquier Administración pública española, las que determina el artículo 19 del RDENI, bajo el título de "aspectos de interoperabilidad relativos a los prestadores de servicios de certificación", que estudiaremos en detalle en relación al tratamiento de los certificados en la política de firma electrónica[35].

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

---

[33] Cfr. la sección 2.1 de este trabajo.

[34] Nótese que es el RDLAE (2009) el que concreta este instrumento, ya que la LFE sólo se había referido al órgano que las aprobaba, sin detallar el tipo de norma.

[35] Véase el capítulo 6.4 de este trabajo.

seguridad pública o a la defensa nacional se regirá por su normativa específica", previsión legal que no resulta aplicable al objeto de este estudio, por lo cual remitimos a su estudio en la doctrina general.

1.4.2 La verificación del cumplimiento de las condiciones adicionales: ¿por qué no se ha establecido un sistema voluntario de certificación de la actividad de los prestadores?

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[36] y de Industria, Turismo y Comercio[37] […] 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[38].

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.

Y, por supuesto, habría que estar a lo que determinen los correspondientes reglamentos que puedan dictar otras Administraciones Públicas que establecen

[36] Esta competencia, en la actualidad, correspondería al Ministerio de Hacienda y Administraciones Públicas.

[37] Esta competencia, en la actualidad, correspondería al Ministerio de Industria, Energía y Turismo.

[38] En especial si se estableciesen – y parece que resultaría conveniente, al menos desde la perspectiva de facilitar el desarrollo de la industria – condiciones generales adicionales válidas en el ámbito de todas las Administraciones Públicas, como de hecho veremos podemos entender que ha sucedido con la aprobación del RDENI.

condiciones adicionales.

Como alternativa, se podría haber establecido un sistema de certificación de la actividad del prestador de servicios de certificación, definido legalmente 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", en el artículo 26.1 LFE.

Este procedimiento no se prevé como 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.

Por lo tanto, 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[39]), que regula la infraestructura acreditable para la calidad.

El segundo grado se corresponde con la definición de unos requisitos y con la

[39] Modificado por Real Decreto 411/1997, de 21 de marzo (BOE núm. 100, de 26/04/1997), por Real Decreto 338/2010, de 19 de marzo (BOE núm. 84, de 07/04/2010) y por Real Decreto 1715/2010, de 17 de diciembre (BOE núm. 7, de 08/01/2011).

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 DFE, 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, y constituir un referencial de control para regular y verificar el cumplimiento de las condiciones adicionales que se encuentren justificadas en dicho escenario.

En caso de existir un sistema voluntario de certificación de la actividad de los prestadores[40], 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 "voluntaria"[41], 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[42].

[40] Sistema voluntario de acreditación, en terminología de la DFE.

[41] Cfr. DUMORTIER et al., 2003: p. 149 indican que la obligación de obtener una certificación del servicio infringe la DFE porque la adherencia al sistema deja de ser libre y voluntaria, y porque reduciría de forma desproporcionada la competencia en los servicios de certificación.

[42] En el proyecto PEPPOL se ha estudiado detalladamente el empleo de niveles de confianza en sistemas de certificación, valorándose los sistemas certificados (sic. acreditados) de forma superior a los

Y dado el previsible isomorfismo entre el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica y el futuro Esquema Judicial de Interoperabilidad y Seguridad[43], podemos anticipar la extensión[44] de esta técnica, defectuosa en nuestra opinión, al procedimiento judicial electrónico[45].

De momento, quizá por influjo de la regulación europea sobre la Ventanilla Única, contenida principalmente en la Decisión 2009/767/CE de 16 de octubre de 2009, modificada por 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[46], pero en nuestra opinión puede ser muy recomendable, y por ello se puede valorar positivamente que la Propuesta de Agenda Digital para España incluya una medida específica que parece apuntar en esta línea.

---

simplemente supervisados.

[43] El isomorfismo es un término matemático que describe la correspondencia biunívoca entre dos estructuras algebraicas que conserva las operaciones. En este contexto, por isomorfismo entre los dos Esquemas nos referimos al hecho de que la sintaxis y semántica básicas de los vocabularios en XML de intercambio de datos y documentos de los Esquemas pretenderán ser intercambiables, a efectos de lograr la tan anhelada interoperabilidad, sin perjuicio de que sea más una aspiración que un objetivo plenamente realizable en la actualidad.

[44] Y por otra parte, MARTÍNEZ GUTIÉRREZ, 2012, pp. 313 y ss. recuerda la aplicación subsidiaria de la LAE y sus normas de desarrollo en aquellas cuestiones de interoperabilidad no previstas en la LUTICAJ (cfr. disposición adicional octava de la LUTICAJ).

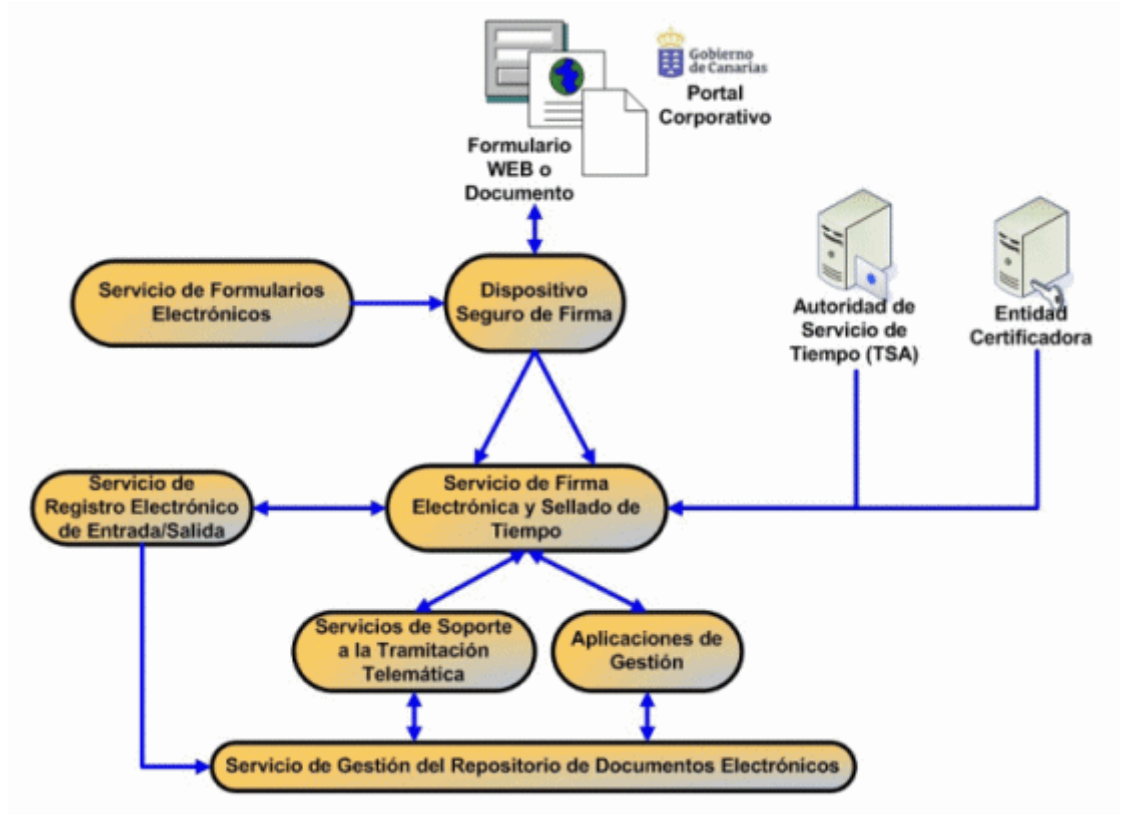
[45] En cambio, se hubiera podido crear un sistema voluntario de certificación, cuya entidad de certificación podría haber sido designada por el Comité técnico estatal de la Administración judicial electrónica, en cumplimiento de aspectos de prestación de servicios de certificación para el procedimiento judicial electrónico, regulados por el Esquema Judicial de Interoperabilidad y Seguridad (cfr. artículos 49 y 51 de la LUTICAJ), y ofrecer una garantía de cumplimiento especialmente reforzada, sin interferir en el funcionamiento del mercado (cfr. ALAMILLO DOMINGO, 2012: p. 449).

[46] De todos modos, actualmente, en el Estado español, no disponemos de ninguna entidad certificadora formalmente acreditada dentro del sistema industrial, como se puede ver en la web de la Entidad Nacional de Acreditación (ENAC). Por este motivo, los únicos sistemas de certificación de prestadores de servicios de certificación disponibles hoy en día son las auditorías hechas por entidades acreditadas o cualificadas de acuerdo con sistemas absolutamente privados, como WebTrust, que ofrece el Instituto de Auditores-Censores Jurados de Cuentas de acuerdo con un contrato de licencia con los Institutos de Auditoría norteamericano y canadiense (AICPA y CICA, respectivamente) y que tiene un gran reconocimiento en el sector privado, y más recientemente, el sello de confianza de prestadores de servicios de certificación de AMETIC, notificado a la Comisión Europea de acuerdo con el procedimiento del artículo 11 de la Directiva de firma electrónica, como sistema voluntario de certificación. Mientras que el primero se basa en estándares propios del sector financiero producidos en EEUU por el comité X9.79 de ANSI, el segundo se basa en estándares europeos, específicamente diseñados para dar cumplimiento a la Directiva 99/93/CE, de firma electrónica y, en particular, para asegurar la calidad en la expedición de certificados reconocidos de firma electrónica (Cfr. ALAMILLO DOMINGO y URIOS APARISI, 2010: pp. 694 y ss).

Así, dentro del objetivo 4.1, referido al impulso del mercado de los servicios de confianza, se ha previsto el "refuerzo de la capacidad supervisora de la Administración, impulsando procesos de auditoría y certificación y asegurando su armonización y el reconocimiento mutuo con las iniciativas europeas", si bien habrá que esperar a la concreción de esta medida para proceder a su valoración definitiva.

2 LA FIRMA ELECTRÓNICA EN LA RELACIÓN ELECTRÓNICA CON LA ADMINISTRACIÓN

Como hemos visto anteriormente, la firma electrónica ha constituido, y sigue siendo, un elemento fundamental en la arquitectura de la Administración electrónica. Como se puede ver en el siguiente diagrama[47], la relación electrónica a través de Internet se construye en gran medida sobre este instrumento:



Quizá por ello se advierte en la legislación de Administración electrónica una amplia regulación de la firma electrónica; de esta forma, tanto la LAE como la LUTICAJ constituyen *leges speciales* en materia de firma electrónica con respecto a la LFE, *lex generalis*, tanto en lo que respecta a la creación de nuevas tipologías de certificados[48]

[47] Cfr. http://moyif.blogspot.com.es/2011/04/firma-electronica.html (última visita: 20/07/2012).

[48] En el ámbito del procedimiento administrativo, el artículo 13.3, en relación con los artículos 17 y 18.1.a) de la LAE, crea dos tipos de certificados, de uso especializado para la sede electrónica y la actuación administrativa automatizada, respectivamente; mientras que en el judicial, el artículo 14.3, en relación con los artículos 18 a 20 de la LUTICAJ, crea dos tipos de certificados, de uso especializado para

como al establecimiento de normas concretas sobre el uso de la firma electrónica en el procedimiento administrativo o judicial, respectivamente.

Esta legislación especial constituye realmente el marco donde se ha desarrollado el uso de la firma electrónica en España, de forma similar a cómo sucede en la Unión Europea, que ha adoptado el uso de la firma electrónica especialmente en el ámbito de la denominada Ventanilla Única de la Directiva de Servicios, así como en la contratación pública electrónica o, hasta tiempos recientes, de la facturación electrónica[49].

2.1 ¿EXISTE UN DERECHO DE ADMISIÓN DE LA FIRMA ELECTRÓNICA?

2.1.1 Los derechos a obtener y emplear la identidad y firma electrónica

La LAE incluye, por primera vez, en su catálogo de derechos, el de "obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública", que recoge el apartado g) del artículo 6.2 de la citada LAE.

Esta inclusión del "derecho a la identidad electrónica" debe relacionarse con la proyección a Internet de los derechos de la personalidad, de forma que se produce una extensión del clásico derecho al nombre, reconvirtiéndose en el derecho a la actuación

---

la sede electrónica judicial y para la actuación judicial automatizada, respectivamente. Como se puede ver, el paralelismo entre la LAE y la LUTICAJ es, en este punto, muy elevado.

[49] La Directiva 2001/115/CE imponía el uso de la firma electrónica avanzada como una de las alternativas para la autenticación en la remisión de las facturas electrónicas, pudiendo los Estados miembro elevar el requerimiento hasta la firma electrónica reconocida, requisito que se mantiene en la Directiva 2006/112/CE, del Consejo, de 28 de noviembre, relativa al sistema común el impuesto sobre el valor añadido, hasta la aprobación de la Directiva 2010/45/UE, de 13 de julio, que modifica el artículo 233 para indicar que “cada sujeto pasivo determinará el modo de garantizar la autenticidad del origen, la integridad del contenido y la legibilidad de las facturas”, pudiendo emplear incluso pistas de auditoría

por vía electrónica, como presupuesto del derecho a la relación electrónica de los ciudadanos con las Administraciones Públicas, que reconoce de forma plena el artículo 6.1 de la LAE.

El derecho a la identidad electrónica se relaciona, además, con el derecho a la igualdad en el acceso electrónico a los servicios públicos, indicado en el apartado c) del artículo 6.2 de la LAE, puesto que sólo las personas con identidad electrónica van a poder ejercitar de forma plena su derecho a la relación electrónica con las Administraciones Públicas, de modo que resulta exigible a dichas Administraciones Públicas el establecimiento de las políticas públicas adecuadas para el suministro de la identidad electrónica y de la firma electrónica a los ciudadanos, y prevenir posibles tratos discriminatorios derivados del sistema de firma electrónica empleado (COTINO HUESO, 2010: pp. 293 y 294).

Uno de los ejes esenciales de este derecho a la obtención de la identidad es, como ya hemos avanzado anteriormente, el suministro del DNI electrónico, que, de hecho es obligatorio en cuanto al soporte físico, pero voluntario en cuanto a los certificados que contiene[50].

Además, al no cubrir el DNI electrónico a todos los ciudadanos[51], no puede hoy ser el único eje de la política pública de identidad electrónica, sino que debe completarse mediante otros sistemas suministrados, en algunos casos de forma gratuita para los ciudadanos, por las Administraciones.

Quizá en atención a ello, el artículo 6.2.h) de la LAE también prevé el derecho a "la

---

fiables.

[50] Cfr. artículo 9 del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica. En este sentido, la sección 4.4.1 de la Declaración de Prácticas de Certificación de la Policía Nacional confirma que "la activación de las funcionalidades electrónicas del DNI tendrá carácter voluntario, por lo que el ciudadano podrá solicitar la revocación de los certificados emitidos como parte del proceso de expedición. Si el usuario no manifiesta la intención de revocar dichos certificados tras la expedición, se dará por confirmada la aceptación de los mismos, así como de sus condiciones de uso, independientemente que se hayan obtenido tras la primera inscripción, en las renovaciones presenciales o en la expedición de duplicados".

[51] Dado que únicamente pueden obtener el DNI electrónico los nacionales españoles, pero no los extranjeros con residencia legal.

utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas".

En concreto, cabe inscribir aquí la emisión de certificados en software a todos los ciudadanos, tarea que actualmente realizan los cuatro prestadores públicos que operan en España, siempre en régimen de libre concurrencia; a saber, la FNMT-RCM, la ACCV (Comunidad Valenciana), el IZENPE (País Vasco) y CATCert (Catalunya), estimándose imprescindible esta actividad al menos mientras el Estado no arbitre una Tarjeta de Residencia Electrónica que asegure la obtención de identidad y firma electrónica por los ciudadanos que no ostentan la nacionalidad española.

Asimismo debemos considerar también otros mecanismos criptográficos asimétricos no basados en certificados electrónicos, o mecanismos criptográficos simétricos, o incluso mecanismos no basados en criptografía.

En desarrollo de los anteriores derechos, que a juicio de COTINO HUESO, 2010: p. 198, supone el reconocimiento de posiciones jurídicas nuevas y propias a la naturaleza del contexto digital, más allá de los esfuerzos por mantener y proyectar los derechos previamente reconocidos al entorno electrónico[52], 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.

[52] Véase también COTINO HUESO Y MONTESINOS GARCÍA, 2012: p. 184, en relación a la LUTICAJ.

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."

En sentido análogo, también la LUTICAJ ha establecido, en su artículo 4.2.f), el derecho de los ciudadanos a "utilizar los sistemas de identificación y firma electrónica del documento nacional de identidad o cualquier otro reconocido para cualquier trámite electrónico con la Administración de Justicia en los términos establecidos por las leyes procesales", y en su artículo 6.1.d), el derecho de los profesionales del ámbito de la Justicia a "utilizar los sistemas de firma electrónica del Documento Nacional de Identidad o cualquier otro reconocido, siempre que dicho sistema le identifique de forma unívoca como profesional[53] para cualquier trámite electrónico con la Administración en los términos establecidos por las leyes procesales".

Adicionalmente, 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".

Sistemas que 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

[53] Nótese la diferencia de tratamiento en cuanto al sistema de firma electrónica considerado admisible para los ciudadanos y para los profesionales. Puesto en el contexto de los sistemas de firma electrónica avanzada basada en certificado electrónico reconocido, se aprecia que en el primer caso el legislador se está refiriendo a certificados individuales (de persona física, de persona jurídica o de entidad sin personalidad jurídica); mientras que en el segundo sólo se refiere a certificados individuales y, además, con un atributo específico. Para COTINO HUESO Y MONTESINOS GARCÍA, 2012: p. 187, la "diferencia se explica por las limitadas cualidades del DNI electrónico".

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."

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[54] – 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[55], exigible siempre que se cumplan las condiciones legales establecidas en la normativa aplicable[56].

[54] MARTÍN DELGADO, 2012: pp. 554 y 555, opina que las personas jurídicas y las entidades sin personalidad jurídica no gozan en la LUTICAJ del derecho a la admisión de sus sistemas de firma electrónica, debido a la omisión de una definición de ciudadano que las incluya, a diferencia de la LAE, omisión que considera "muy criticable, por cuanto supone retroceder y no incorporar a este ámbito el avance producido en el marco de las relaciones jurídico-administrativas", si bien también reconoce que "las mismas actuarán en juicio normalmente asistidas por abogado y procurador, con lo que la omisión tiene efectos limitados".

[55] En este sentido, resulta clarificadora la exposición de motivos de la LAE cuando indica que "también se establece la obligación para cualquier Administración de admitir los certificados electrónicos reconocidos en el ámbito de la Ley de Firma Electrónica", manifestación menos asertiva en la exposición de motivos de la LUTICAJ, que sencillamente alude a que, en cuanto a los ciudadanos, "se contempla la posibilidad de uso de diversos sistemas de firma electrónica además del incorporado al Documento Nacional de Identidad", diferencia de intensidad que puede venir motivada por el diferente nivel de madurez tecnológica en la Administración de Justicia, o porque ya no considere el legislador tan importante afirmar este derecho, más ampliamente extendido que en el momento de redacción de la LAE.

[56] Que incluyen los requisitos establecidos directamente en las propias LAE y LUTICAJ, así como las condiciones adicionales que, según hemos visto, se puedan establecer para salvaguardar las garantías de cada procedimiento.

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 dela 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[57] 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 en nuestra opinión ello no implica que la decisión de admitir o no un sistema de firma electrónica sea puramente discrecional 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.

En ambas leyes, resulta llamativo que no se garantice ningún tratamiento privilegiado[58] en relación con 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

[57] No así la LUTICAJ, que no contiene esta referencia "a lo que cada Administración determine", sino una referencia a la sujeción estricta a las leyes procesales.

[58] Hay diversas razones, sin embargo, que avalan este tratamiento, en especial a la luz de la normativa dela Unión Europea que, en el marco de la Directiva de servicios, impone a los Estados miembros la obligación de admitir los sistemas de firma electrónica avanzada basada en certificado supervisado, como tendremos ocasión de analizar detalladamente.

un volumen masivo de unidades de DNI electrónico[59], que es precisamente una firma electrónica reconocida, y de hecho especialmente segura.

De hecho, puede indicarse que el sólo DNI electrónico recibe un tratamiento privilegiado, derivado de la obligación general de aceptación[60] 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[61]. Las referencias que se realizan en los artículos 13.2.a) 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[62], 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[63] y la LUTICAJ[64], y que ha obligado a replantear

---

[59] En mayo de 2012 se han emitido 28.532.108 DNI electrónicos, de acuerdo con el Boletín de indicadores de Administración electrónica del Observatorio de Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas correspondiente a junio de 2012.

[60] En otro lugar nos hemos referido a los efectos del DNI electrónico sobre el mercado de la certificación. Cfr. ALAMILLO DOMINGO y URIOS APARISI, 2003. No hemos alterado ni un ápice esta opinión, y efectivamente la experiencia ha demostrado la inviabilidad de comercializar certificados de persona física, y la desaparición total de la competencia en este caso. Sólo iniciativas públicas financiadas a cargo del presupuesto público – en particular el certificado Clase 2 CA o de la FNMT-RCM o el certificado idCAT de CATCert – pueden hoy convivir con el DNI electrónico, y en nuestra opinión sencillamente por su mayor facilidad de uso, que ciertamente deriva de su menor seguridad técnica. En sentido similar, DUMORTIER *et al.*, 2003: p. 149 indican que el establecimiento, por las Administraciones Públicas, de servicios de certificación para su uso exclusivo en los procedimientos administrativos resulta posible, pero que el uso de dichos servicios para otros usos resulta inadmisible en términos de competencia efectiva, constituyendo una barrera al mercado interior.

[61] Nótese que cuando el legislador se refiere al DNI electrónico no lo cualifica nunca de sistema "admitido", cosa que sí hace de forma expresa cuando se refiere a los restantes sistemas de firma electrónica avanzada. Además, en la LUTICAJ el legislador se refiere, en los artículos 4.2.f) y 6.2.d) al derecho a "utilizar los sistemas de firma electrónica del Documento Nacional de Identidad o cualquier otro reconocido", lo cual sólo puede generar mayor confusión en este ámbito.

[62] Resulta digno de mención notar que en la LUTICAJ no se hace uso de esta expresión reforzada en relación con el uso del DNI electrónico, sin perjuicio de ser igualmente un instrumento de firma electrónica privilegiado frente a los restantes en su misma categoría, que es la firma electrónica reconocida.

[63] Artículo 4, apartados f) y g), y artículo 27.5, ambos de la LAE.

[64] Aunque dichos principios no se mencionan de forma explícita en la LUTICAJ, cfr. artículo 33.4 de la propia LUTICAJ, análogo al correlativo 27.5 de la LAE.

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.

La Agenda Digital para Europa considera de forma muy explícita, en este sentido, que "como las soluciones serán múltiples, es necesario que la industria, respaldada por medidas políticas – en particular los servicios de administración electrónica – garantice la interoperabilidad sobre la base de unas normas y de unas plataformas de desarrollo abiertas"[65], así como la necesidad de establecer una estrategia europea sobre la gestión de identidad, incluidas propuestas legislativas sobre la tipificación de delitos de usurpación de identidad, sobre la identidad electrónica y sobre los sistemas de autenticación seguros[66], que debería estar finalizada en 2012.

2.1.2 Los requisitos para la 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, cuyos caracteres generales hemos expuesto anteriormente 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.

[65] COM (2010) 245 final/2: p. 13.

[66] COM (2010) 171 final: p. 41.

2.1.2.1 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, como hemos visto, 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; verificación del cumplimiento que puede resultar bastante compleja, especialmente porque, como hemos visto, 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[67] y en forma de Lista de Servicios de Confianza (o TSL[68]) firmada electrónicamente por el citado Ministerio.

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

[67] Dicho servicio de consulta se encuentra disponible en la sede electrónica del Ministerio, accesible en la dirección https://sedeaplicaciones2.minetur.gob.es/prestadores/ (última visita: 27/06/2012).

[68] Trust Service List española, disponible en la sede electrónica del Ministerio, accesible en la dirección http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/Prestadores.aspx, y que a su vez se encuentra referenciada en la TSL de la Unión Europa, publicadas en cumplimiento de lo establecido en la Decisión de la Comisión 2009/767/CE, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas (última visita: 27/06/2012). Cfr. la sección 6.4.2 de este trabajo.

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[69].

Como hemos visto, esta opción es la más segura jurídicamente en cuanto a la efectiva admisión, pero no la única, por lo que en nuestra opinión se deberá hacer uso de la potestad discrecional de admisión de otros sistemas de firma electrónica prevista legalmente.

Finalmente, como hemos ya indicado *supra*[70], el establecimiento de un sistema voluntario de certificación de la actividad de prestación de servicios de certificación de firma, específicamente diseñado para la Administración electrónica, resultaría muy útil para facilitar la verificación del cumplimiento de la LFE y de las condiciones adicionales aplicables al uso de la firma electrónica en el sector público.

2.1.2.2 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.

---

[69] Incluso aún en el caso de un Ministerio que realmente es meticuloso en los procedimientos de comunicación de inicio de actividad, lo cierto es que su capacidad de "no darse por notificado" o de influir de forma profunda en la configuración del servicio de certificación objeto de la comunicación, resulta ciertamente limitada, en ausencia de un Reglamento de desarrollo de la LFE que concrete los detalles técnicos de la actividad de prestación de servicios de certificación.

[70] Cfr. la sección 1.4.2 de este trabajo.

Sin embargo, como hemos estudiado, en realidad nada más alejado de la realidad: la LFE permite la existencia de sistemas de firma electrónica que muy laxamente identifican a los firmantes[71]. Sólo los certificados reconocidos, como hemos visto, ofrecen realmente una garantía estricta sobre la identidad de los firmantes[72].

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 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.

[71] Asimismo, existen otros sistemas de firma electrónica, ordinaria o avanzada, que no se basan en certificados electrónicos, pero que pueden resultar útiles y seguros para el procedimiento administrativo.

[72] En este sentido, nos resulta llamativa la crítica feroz de BOIX PALOP (2010: p. 320), por ciento refiriéndose a diversas alteraciones de la neutralidad tecnológica, cuando indica que "la continuada y reiterada tendencia a pedir firma digital vigente hasta la fecha demuestra, sin dudas, un grado de exigencia mucho mayor en el procedimiento electrónico que en el ordinario. […] Por extraños motivos asociados a un supuesto 'miedo al fraude' que se asocia, sin que se sepa muy bien por qué, a las actuaciones por vía electrónica, […] la fehaciencia parecía en todo casi indispensable. […] tardaremos un tiempo en desterrar totalmente la práctica de 'hiperproteger' el procedimiento administrativo de manera desproporcionada y en todo caso muy superior a la exigida en otros casos"; posición con la que sólo estamos parcialmente de acuerdo.

Mientras que la LAE no parece apostar por el uso de la firma electrónica reconocida ni en el caso de los ciudadanos[73] ni en el del personal al servicio de la Administración[74], en cambio la LUTICAJ parece adoptar el criterio contrario, apuntando a la necesidad de uso de la firma electrónica con carácter general[75].

También el RDL 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, indica en su disposición adicional decimosexta que "todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas que tengan efectos jurídicos y se emitan tanto en la fase preparatoria como en las fases de licitación, adjudicación y ejecución del contrato deben ser autenticados mediante una firma electrónica reconocida de acuerdo con la Ley 59/2003, de 19 de diciembre, de Firma Electrónica".

- 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[76].

- En tercer lugar, se debería evaluar el nivel de seguridad[77] del activo documental

[73] Cfr. ALAMILLO DOMINGO y URIOS APARISI: 2010, pp. 665 y ss.

[74] Cfr. LINARES GIL, 2010: p. 439.

[75] El artículo 27.3 de la LUTICAJ exige la firma electrónica reconocida (y la fecha electrónica) como condición para el documento público judicial electrónico; mientras que el artículo 36.3 de la misma LUTICAJ exige a los profesionales el uso de la firma electrónica reconocida para la presentación electrónica de demandas y otros escritos (por cierto, nótese que el Informe del CGPJ al anteproyecto de la LUTICAJ se muestra en contra de la exigencia de firma electrónica reconocida a los profesionales, por considerarla excesivamente rigurosa); asimismo, los artículos 146 y 147 de la LEC requieren la firma electrónica reconocida del secretario judicial para la documentación de las actuaciones en soporte apto para la grabación y reproducción; y los artículos 267 y 268 de la LEC también exigen la firma electrónica reconocida para la aportación de documentos públicos y privados en forma de copia digitalizada. Cfr. MARTÍN DELGADO, 2012: pp. 552 y 553, en defensa del empleo de la firma electrónica reconocida.

[76] Motivo por el cual la Administración no puede impedir el empleo de dichos sistemas, de suerte que por ejemplo, un sistema de firma electrónica basado únicamente en el empleo de contraseñas resultaría contrario a la LAE y a la LUTICAJ.

[77] Abordamos esta cuestión con detalle *infra*, en las secciones 5.4 y 6.3.3 de este trabajo.

de acuerdo con las dimensiones de seguridad del Esquema Nacional de Seguridad[78], 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 Nacional de Interoperabilidad [79] que resulten aplicables al sistema de firma electrónica en cuestión[80].

- 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[81].

Los sistemas de firma electrónica evaluados[82] de esta forma resultarán, en principio, adecuados para la actuación de que se trate[83].

2.1.3 Las reglas legales de 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, en relación a aquellos sistemas que se

[78] Cuando se apruebe, en el ámbito judicial, será aplicable el Esquema Judicial de Interoperabilidad y Seguridad.

[79] Cuando se apruebe, en el ámbito judicial, será aplicable el Esquema Judicial de Interoperabilidad y Seguridad.

[80] Y, en particular, las condiciones de la denominada "política de firma electrónica y de certificados", redactada de acuerdo con los requisitos de mínimos establecidos por la Norma Técnica de Interoperabilidad correspondiente, que estudiamos *infra*, capítulo 3.

[81] Como ya hemos indicado anteriormente, en general se considera necesario restringir el uso de los certificados con seudónimo en el procedimiento electrónico, si bien puede resultar perfectamente aceptable en otras circunstancias, como la participación.

[82] En su Informe al anteproyecto de la LUTICAJ, el CGPJ se considera órgano competente para la determinación del nivel adecuado de firma para cada trámite (cfr. conclusión séptima).

[83] De aplicarse estos criterios en el ámbito de la Administración electrónica de Justicia, se obtendrá un resultado consistente con los sistemas de firma empleados en el contexto de la LAE, algo deseable porque, como establece el artículo 47.3 de la LUTICAJ, en la elaboración del Esquema Judicial de Interoperabilidad y Seguridad se tendrá en cuenta lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad, así como las recomendaciones de la Unión Europea, entre otros criterios.

basan en certificados electrónicos. En este sentido, la LAE y la LUTICAJ autorizan[84] 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[85]. 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", previsión 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[86] hasta algoritmos de autenticación de mensajes basados en contraseñas[87]. También se emplean algoritmos asimétricos, de firma digital, pero sin

[84] Artículo 13.2.b) y 14.2.b) respectivamente.

[85] La legislación española parece en este punto bastante correcta. DUMORTIER et al., 2003: p. 149, consideran que una legislación que exigiese en términos estrictos el uso de sistemas de firma electrónica reconocida sería incompatible con la DFE. Parece que esta posición ha sido acogida con carácter general en el Derecho comunitario y español.

[86] GRUBER *et al*., 2006: pp. 110-115, muestran un sistema de bolígrafo digitalizador capaz de verificar la autenticidad de una firma manuscrita, que puede cualificar perfectamente como sistema de firma electrónica avanzada. Cfr. también BASHIR y KEMPF, 2009.

[87] Sistemas como HMAC basado en clave maestra derivada de contraseña, por ejemplo.

uso de certificados electrónicos, incluso en proyectos de ámbito europeo[88].

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 de 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 AAPP, 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".

En nuestra opinión, el 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[89]. Obviamente, sólo los certificados electrónicos reconocidos garantizan una calidad en la identificación del firmante[90], 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

[88] Por ejemplo, en el proyecto europeo PEPPOL las claves de firma electrónica de los Estados participantes se gestionan mediante su publicación en un depósito electrónico. Las firmas electrónicas generadas se verifican mediante el protocolo XKMS.

[89] Cfr. MARTÍN DELGADO, 2010: pp. 495 y ss., quien indica, por una parte, que la LAE no contiene ninguna disposición que regule las condiciones que deben cumplir los certificados para poder ser admitidos, si bien posteriormente analiza las condiciones del artículo 21 de la LAE, que encuentra excesivamente vagas. Cfr. también MARTÍN DELGADO, 2012: pp. 518 y ss. en relación con el tratamiento de esta cuestión en la LUTICAJ.

[90] Esta manifestación es cierta incluso en el caso de certificados reconocidos con seudónimo, ya que el prestador del servicio de certificación conoce la identidad real.

Administración debiera pagar un coste al prestador[91].

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[92], si bien genera mayor inseguridad que deban hacerlo "en condiciones que resulten tecnológicamente viables[93]", 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".

---

[91] En este caso se plantearían problemas de diversa índole, especialmente en el caso de prestadores privados de servicios de certificación: ¿quién decidiría los precios?, ¿existiría un debe de admitir certificados a todos los prestadores? o ¿serían aceptables modelos de negocio como el de la FNMT-RCM, en el que las Administraciones usuarias abonan un coste ligado al volumen de población residente, en lugar de pagar por el número de certificados electrónicos efectivamente expedidos? La aplicación de la propia legislación de contratos del sector público, en nuestra opinión, impondría la obligación de tratar esta admisión como una cuestión contractual sujeta a la ley, cuyo tratamiento resultaría extraordinariamente complejo. En nuestra opinión, en este escenario sencillamente el derecho de admisión sería sencillamente inviable y quedaría vacío de contenido.

[92] Resulta muy interesante, en este sentido, la reflexión de ORTEGA DÍAZ, 2008: p. 257, en el sentido de considerar que la obligación del prestador de suministrar copias de los certificados expedidos, y la información de estado de vigencia de los mismos, "tiene una base legal (artículo 18.d LFE) y es que se trata de una prestación consustancial al tipo contractual. […] Y ello es así porque la obligación del certificador a conceder el acceso a los terceros, para que verifiquen el contenido del certificado electrónico, es una obligación al servicio de la certificación. De nada sirven todas las obligaciones si ésa no se cumple. La utilidad del servicio no se traslada al usuario del servicio (suscriptor) pues no se generará la confianza que hará posible la fiabilidad de la firma electrónica ante los ojos de los terceros".

[93] La explicación a este requisito deriva a la ausencia de normativa legal o reglamentaria que concrete, desde un punto de vista técnico, las obligaciones de suministro de información de estado de certificados. Dada la diversidad de mecanismos técnicos disponibles, incluyendo listas de revocación de certificados (CRL), servicios en línea de información de estado de certificados (OCSP, SCVP, XKMS) o incluso depósitos web de consulta manual, parece necesario prever alguna restricción en este sentido.

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[94] 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.

Como ejemplo de reconocimiento mutuo, se puede mencionar el Convenio de cooperación tecnológica entre el Ministerio de Justicia y el Departamento de Justicia de la Generalitat de Catalunya para la implantación y ejecución de la presentación telemática de escritos y notificaciones – sistema LexNET – en las oficinas judiciales de Cataluña, firmado el 5 de mayo de 2006, y publicado por Resolución 2006/3165/JUS, de 28 de septiembre, mediante el cual se admiten en el ámbito de cada parte los certificados utilizados por la otra parte, de forma recíproca y sin coste alguno, técnica que supone una salida al "problema" del modelo de negocio de la FNMT-RCM[95], por causa del que los usuarios de certificados CERES se encuentran excluidos del “derecho” de admisión.

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

[94] Más habitualmente, por criterio práctico, el prestador que expide el certificado será el que solicite la “admisión” de su sistema de firma electrónica, dado que incrementa el valor de su propio servicio.

[95] Como es conocido, en el modelo de negocio de la FNMT-RCM los terceros verificadores de certificados deben adherirse a un convenio (si son entidades públicas) o a un contrato (si son ciudadanos o empresas), y abonar un precio por el derecho a hacer uso del certificados; de forma que los terceros sin convenio no pueden ni siquiera acceder a la información de estado de vigencia de los certificados. Los restantes prestadores de servicios de certificación, por el contrario, únicamente cobran al firmante por el suministro del certificado y, en su caso, del dispositivo de firma, resultando gratuito el acceso a la información de estado para todos los verificadores. Adicionalmente, cfr. COELLO DE PORTUGAL, 2003: pp. 99 y ss., que critica el uso de la figura del convenio administrativo por parte de la FNMT-RCM para la prestación de sus servicios, que califica de contrario a la legislación de contratos.

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 aquéllas".

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, como hemos tenido ocasión de analizar anteriormente; previsión que resulta razonable, dada la ausencia de garantía respecto a la identificación en los certificados no reconocidos[96].

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[97].

A mayor abundamiento, la información a suministrar debe serlo bajo principios de reconocimiento mutuo y reciprocidad, y sin que suponga coste alguno para las Administraciones competentes, punto en el que el artículo 22.1 de la LUTICAJ se aleja de la LAE, mediante una redacción imprecisa y desafortunada, en particular por la mezcla de dos casos que resultan claramente heterogéneos. Efectivamente, resulta sencillamente absurda la aplicación de los principios de reconocimiento mutuo y reciprocidad a la admisión de los certificados cuando la misma es solicitada por los ciudadanos o por los prestadores que les suministran certificados[98].

---

[96] Y por supuesto, igualmente en el caso de los sistemas de firma electrónica que ni siquiera emplean certificados electrónicos.

[97] La cuestión, a nuestro juicio, puede y debe ser resulta en sede del Esquema Judicial de Interoperabilidad y Seguridad, en particular acudiendo a la figura de la política de firma electrónica y de certificados, de forma análoga a como se ha tratado la cuestión en el ámbito de la Administración electrónica (Cfr. la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública).

[98] Sí, en cambio, puede resultar aceptable la norma en relación con los certificados expedidos a magistrados, jueces, secretarios judiciales, fiscales, abogados del estado y funcionarios al servicio de la

En definitiva, y como hemos expuesto en otro lugar, 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 reconocido 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, supuestamente dentro de la libre concurrencia que exige la LFE (ALAMILLO DOMINGO Y URIOS APARISI, 2010: p. 665 ALAMILLO DOMINGO Y URIOS APARISI, 2010: p. 665).

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.

2.1.4 ¿Pueden ser objeto de admisión otros sistemas de firma electrónica?

Como hemos visto, 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.

Además, el artículo 16.1 de la LAE, que por cierto 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[99], también permite a la Administración la admisión de mecanismos de identidad expedidos por terceros, mediante la técnica de la "delegación de la autenticación", en cuyo caso la Administración se acoge al uso de sistemas de identificación operados por terceros, incluidos prestadores privados, como Google o Facebook.

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[100].

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.

Asimismo, el empleo de mecanismos basados en federaciones de identidad y atributos puede ser apropiado en muchos procedimientos administrativos, donde realmente lo único que se requiere acreditar es un rol o atributo, sin que sean muy relevantes los datos de identidad raíz, ni mucho menos, imprescindible el empleo de un identificador universal[101].

Por ejemplo, resulta perfectamente aceptable la simple acreditación del "rol" de

---

[99] A título de ejemplo podemos citar la Orden CUL/1132/2011, de 28 de abril, por la que se aprueba el sistema de firma electrónica de clave concertada para actuaciones en el Registro Electrónico del Ministerio de Cultura y se modifica la Orden CUL/3410/2009, de 14 de diciembre de 2009, que regula el Registro Electrónico del Ministerio de Cultura, o la Orden EHA/2219/2010, de 29 de julio, por la que se aprueba el sistema de firma electrónica de clave concertada para actuaciones en la sede electrónica de la Dirección General del Catastro, entre otras.

[100] Se puede acceder a más información en la página web gubernamental http://www.idmanagement.gov/pages.cfm/page/ICAM (última visita: 29/06/2012).

[101] Como ha indicado BARRAT I ESTEVE (2010: p. 825), "descubriremos seguramente que muchas actividades no requieren la revelación completa de una (id)entidad y que muchos objetivos pueden desarrollarse con plenitud manejando única y exclusivamente identidades y atributos. Habremos conseguido, por lo tanto, excluir en ciertas operaciones aquellos datos que albergan mayores peligros para la autodeterminación informativa de los individuos ya que, al ser entificadores, abocan a una inmediata revelación de la entidad del afectado".

vecino, para la actuación electrónica en el ámbito de los mecanismos y procesos participativos que los ayuntamientos deben desplegar: un consejo social de la ciudad de tipo consultivo, presupuestos participativos, mejores canales de comunicación con los ciudadanos aprovechando las TIC, una comisión de sugerencias y reclamaciones para la defensa de los vecinos o peticiones y consultas populares, entre otros[102].

2.1.5 La urgente necesidad de establecer un procedimiento administrativo formalizado para la admisión de sistemas de firma electrónica

Presentado el derecho y las condiciones para la admisión de los sistemas de firma electrónica de los ciudadanos por la Administración, cabe ahora centrarse en la necesidad de un procedimiento para el ejercicio del citado derecho, aspecto que nos parece de importancia capital, y que en la actualidad se encuentra, cuanto menos, insuficientemente tratado.

En el ámbito de la Administración electrónica tributaria, la admisión de sistemas de firma electrónica basada en certificados electrónicos[103] se ha venido configurando como un procedimiento administrativo de carácter decisorio y previo al uso de los certificados emitidos por un prestador de servicios de certificación, que llevan a cabo las Administraciones Públicas tributarias, sus organismos autónomos u otras entidades públicas o empresariales vinculadas[104], y que no parece haber recibido un tratamiento adecuado en el desarrollo de la LAE[105].

La finalidad de un procedimiento de admisión es triple: por una parte, el procedimiento determina la formación y la exteriorización de la voluntad

[102] Véase BORGE *et alia* (2008), por ejemplo, para un análisis explicativo de las experiencias locales de participación, presenciales y electrónicas, en Cataluña.

[103] Como hemos anticipado supra, no existe ninguna experiencia de admisión de sistemas de firma electrónica que no se base en certificado electrónico, ni derecho alguno a la misma.

[104] Cfr. Orden HAC/1181/2003, de 12 de mayo.

administrativa de hacer uso de la firma electrónica; por otra parte, supone que la Administración, que debe pasar a ser usuaria de los servicios de certificación, comprueba que el prestador ha cumplido de manera efectiva los requisitos establecidos en la LFE; finalmente, el procedimiento de admisión puede también servir a la Administración para establecer[106] y, posteriormente, comprobar condiciones adicionales al uso de la firma electrónica aplicables al procedimiento concreto de que se trate[107].

De esta forma, el propio procedimiento de admisión se ha venido tratando como una suerte de condición adicional implícita pero exigible a los prestadores de servicios de certificación, orientada a la comprobación previa del cumplimiento de la legislación de firma electrónica y, en su caso, de las condiciones adicionales[108] del procedimiento que se hayan establecido.

La necesidad de hacer esta comprobación previa ha encontrado, por otra parte, su justificación en el régimen de libre acceso al mercado que consagran el artículo 3.1[109] de la DFE, y el artículo 5.1 LFE, en virtud del cual la prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre concurrencia[110].

---

[105] Tampoco se anticipa que esta cuestión sea adecuadamente tratada en el ámbito de la LUTICAJ.

[106] Cumpliendo con los requisitos que establece la legislación y su normativa de desarrollo, especialmente en materia de aprobación.

[107] Sólo se podrán, sin embargo, establecer condiciones adicionales particulares dado que, como hemos visto anteriormente, el establecimiento de condiciones adicionales generales requiere, al menos en la Administración General del Estado, de una norma reglamentaria.

[108] Por ejemplo, las reglas dictadas en desarrollo de la Orden HAC/1181/2003, incluyen requisitos técnicos detallados que afectan a la información de identidad contenida en el certificado, como la obligación de incluir el Número de Identificación Fiscal español en los certificados, condición que, de hecho, impide de facto la admisión de los certificados expedidos en otros Estados de la Unión Europea a sus nacionales, que no incluyen este código. Esta condición impide, por ejemplo, a un ciudadano alemán relacionarse con la AEAT con un certificado electrónico reconocido expedido conforme a la legislación alemana.

[109] Dicho artículo establece que los Estados Miembros no condicionarán la prestación de servicios de certificación a la obtención de autorización previa.

[110] Al menos parece ser así desde la Orden HAC/1181/2003, de 12 de mayo, porque hasta entonces sólo se admitían los certificados Clase 2 CA de la FNMT-RCM.

No se puede obviar que este régimen de libre acceso a la actividad de prestador de servicios de certificación supone encontrar, en el mercado, prestadores con diferentes niveles de calidad e, incluso, prestadores que sencillamente incumplen la normativa. En el fondo del procedimiento de admisión reside, por lo tanto, una auditoría del prestador de servicios de certificación que en algunos casos se delega, en todo o en parte, a un experto independiente o que puede remitirse a una certificación de la actividad del prestador.

Hay que decir, en cualquier caso, que el procedimiento de admisión no constituye una autorización previa para poder emitir certificados electrónicos al público ni una medida equivalente a ésta, y, caso de que se impongan condiciones adicionales, éstas deben ser objetivas, proporcionadas, transparentes y no discriminatorias.

En el caso de los certificados de persona jurídica y de entidad sin personalidad jurídica, el procedimiento de admisión de certificados es especialmente importante ya que, de acuerdo con el artículo 7.3 de la LFE, los certificados de persona jurídica sólo se podrán utilizar cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones Públicas. En sentido similar, los artículos 15.3 de la LAE y 15 de la LUTICAJ refuerzan la posición de la necesaria admisión previa de los certificados de persona jurídica o de entidad sin personalidad jurídica como condición para su uso en los procedimientos y actuaciones correspondientes.

Sin abandonar aún el ámbito de la Administración electrónica, resulta notable y, a nuestro juicio criticable, que la legislación, ni su posterior desarrollo reglamentario hayan establecido un procedimiento único para la admisión de certificados, al menos para la Administración General del Estado[111].

Más criticable nos resulta aún el hecho de que sencillamente no exista procedimiento ninguno previsto, más allá del ya indicado en el ámbito de actuación de la AEAT, y es que actualmente el Ministerio de Hacienda y Administraciones Públicas, responsable

[111] Podría resultar, en efecto, discutible que un reglamento estatal impusiese los resultados de un concreto procedimiento de admisión a las restantes Administraciones, al menos sin una previsión legal al respecto.

de la plataforma común de verificación, @firma, actúa "de oficio" para configurar técnicamente los certificados en el sistema[112], una vez que el prestador aparece publicado[113] en la sede electrónica del Ministerio de Industria, Energía y Turismo; aunque resulta encomiable, lo cierto es que la ausencia de un procedimiento formalizado de admisión genera inseguridad jurídica, a la par que posible indefensión del ciudadano o del prestador a que interesa la admisión del certificado, especialmente en caso de inadmisión por incompatibilidad técnica.

Como han enseñado GARCÍA DE ENTERRÍA Y FERNÁNDEZ, el procedimiento administrativo es una de las garantías de la posición jurídica del administrado, "en tanto que supone que la actividad de la Administración tiene que canalizarse obligadamente a través de unos cauces determinados como requisito mínimo para que pueda ser calificada como actividad legítima", mientras que "el sistema de recursos contra los actos y disposiciones emanadas de la Administración constituye, en principio, un segundo círculo de garantías, puesto que permite a los administrados reaccionar frente a los actos y disposiciones lesivos a sus intereses y obtener, eventualmente, su anulación, modificación o reforma" (GARCÍA DE ENTERRÍA Y FERNÁNDEZ, 2008b: pp. 451 y ss).

Sin procedimiento formalizado, no existe órgano competente[114], ni solicitud de admisión, ni fases de prueba, alegaciones, audiencia o recurso, ni por supuesto plazos que permitan prever la aplicación del silencio administrativo, lo cual sitúa a un ciudadano, o también a un prestador, cuyo sistema de firma electrónica no sea admitido en la práctica, teniendo derecho a ello[115], en una situación de desventaja y

[112] Esta procedimiento técnico de carga es la plasmación efectiva de la admisión, dado que sin esta configuración, la plataforma no verifica el certificado, devolviendo error y, por tanto, "inadmitiendo" materialmente el uso del certificado.

[113] La publicación se produce una vez el prestador ha comunicado al Ministerio el inicio de su actividad, verificadas las condiciones mínimas por el supervisor.

[114] Problema que puede ser realmente grave atendiendo a la multitud de plataformas de verificación de certificados que se pueden desplegar, por cierto. Además de hecho de no poder determinar si una decisión evidentemente administrativa, y con impacto en el modelo de negocio del prestador o en la esfera de intereses del ciudadano afectado, ha sido tomada por un órgano en ejercicio de su potestad o por un técnico de la Administración.

[115] En particular, en el caso de admisión de un certificado electrónico reconocido que cumpla todas las condiciones del artículo 21.1 de la LAE.

perjuicio – incluso desde la perspectiva patrimonial – que sólo se puede resolver mediante el ejercicio del derecho subjetivo reaccional construido por la más autorizada doctrina (GARCÍA DE ENTERRÍA Y FERNÁNDEZ, 2008b: pp. 44 y ss.), en este caso, por inactividad de la Administración.

A tal efecto, el ciudadano, o prestador de servicios de certificación, que entienda que se conculca su derecho deberá presentar una reclamación ante la Administración actuante, y si en el plazo de tres meses a Administración no hubiera dado cumplimiento a lo solicitado o no hubiera llegado a un acuerdo con los interesados, éstos pueden deducir recurso contencioso-administrativo contra la inactividad de la Administración, según dispone el artículo 29 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, pudiendo, además, solicitar la adopción de medidas cautelares, incluso urgentes, si de la inadmisión se pudieren producir graves perjuicios; en particular, la suspensión del cómputo de los plazos de los procedimientos administrativos que exigen el empleo del sistema de firma electrónica, cuando se imponga obligatoriamente la vía electrónica[116].

En consecuencia, creemos que es necesario y urgente resolver esta cuestión en el ámbito de la Administración electrónica. Como hemos visto al referirnos a las condiciones adicionales al uso de la firma electrónica en el sector público y a la verificación del cumplimiento de la legislación de firma electrónica como requisito para la admisión, se podría organizar esta cuestión mediante un sistema voluntario de certificación de la actividad de los prestadores que se encuentren interesados.

Este mecanismo resultaría apropiado y equilibrado para el establecimiento de unas reglas del juego comunes para todo el territorio español[117], y simplificaría

[116] Dado que la Administración que impone la vía electrónica como obligatoria y no admite el uso del certificado es la misma, parece razonable adoptar medidas cautelares para que el transcurso de los plazos que el ciudadano deja de cumplir por la inadmisión del certificado no le perjudique. Nótese que en caso de no solicitar y obtener esta medida cautelar, el ciudadano deberá obtener otro certificado para no sufrir los perjuicios correspondientes.

[117] Sería necesario, sin embargo, establecer un marco de gobernanza que considerase, no sólo a la Administración General del Estado, sino a los restantes niveles de la Administración, quizá en el marco de la Conferencia Sectorial de Administración Pública, como en el caso de los Esquemas Nacionales de Interoperabilidad y Seguridad, según previsión del artículo 42.3 de la LAE.

enormemente el ejercicio del derecho de admisión, al menos en el caso de los certificados electrónicos reconocidos.

En nuestra opinión, continuaría siendo preciso el establecimiento de un procedimiento, pero el mismo podría contemplar la "admisión automática" cuando se verifique que el sistema empleado por el ciudadano solicitante se encuentra certificado. Para los sistemas que, cumpliendo con los requisitos del artículo 21.1 de la LAE, no se hubiese obtenido la certificación de la actividad, se debería tramitar el procedimiento completo, como hoy sucede en el caso de la admisión en el ámbito tributario.

Y por lo que se refiere a los restantes sistemas de firma electrónica, en los que ni siquiera existe un verdadero derecho de admisión ni condiciones reguladoras de su alcance, la existencia de un procedimiento formalizado resulta, en nuestra opinión, imprescindible para dotar a esta potestad de la Administración, altamente discrecional, de unas mínimas condiciones de seguridad jurídica.

Por estos motivos, y atendiendo a la incluso mayor relevancia del procedimiento judicial electrónico, en nuestra opinión debe también establecerse un procedimiento de admisión de certificados en cada Administración competente en materia de justicia[118], por la mayor proximidad e impacto de dichos procedimientos sobre los derechos del ciudadano[119].

[118] Entendemos, en línea con el Informe del CGPJ al anteproyecto de la LUTICAJ, que sólo los certificados admitidos por las Administraciones competentes en materia de justicia, y para esta finalidad, son objeto de este tratamiento; y no los certificados admitidos por otras Administraciones, o para otros usos.

[119] Los efectos del procedimiento de admisión se extenderían sin problemas a las restantes Administraciones eventualmente receptoras de documentos firmados, en virtud de la regla del artículo 22.1 de la LUTICAJ, y bajo los ya mencionados principios de reconocimiento mutuo y reciprocidad, por lo que se daría cumplida solución a la necesaria seguridad jurídica de todas las partes implicadas: ciudadanos y prestadores, y también las Administraciones competentes.

2.2 EL "RÉGIMEN DE USO" DE LA FIRMA ELECTRÓNICA

En cuanto al empleo de los sistemas de firma electrónica, una vez admitidos, los artículos 12 del RDLAE[120] y 16 de la LUTICAJ establecen dos reglas heterogéneas, agrupadas bajo el epígrafe de régimen de uso de la firma electrónica, que veremos a continuación para, antes de abandonar esta sección, preguntarnos sobre la verificación de la firma como acto administrativo, y revisar la necesidad de empleo de plataformas de verificación.

2.2.1 El mantenimiento de las obligaciones de cumplimentado de los datos identificativos en la documentación

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, una norma que recuerda que incluso en el caso de la identificación plena con firma electrónica (ya que en general se admite el uso de la firma electrónica cuando la misma se base en certificado reconocido, o bien se exige el uso de firma electrónica reconocida) sigue siendo necesario, al menos potencialmente, el cumplimentado manual de los datos de identidad en el correspondiente formulario o documento administrativo o judicial.

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

[120] Recordemos que sólo aplicable en el ámbito de la Administración General del Estado.

sistemas de firma electrónica que no se basan en certificados electrónicos[121], 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[122].

2.2.2 La autorización de tratamiento de datos personales para la verificación de la firma

En segundo lugar, los artículos 12.2 del RDLAE y 16.2 de la LUTICAJ establecen que los órganos de la Administración 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.

En el caso de los sistemas de firma electrónica basada en certificados electrónicos, la LFE contiene, en su artículo 17, algunas previsiones (Cfr. BALLESTEROS MOFFA, 2005: pp.

[121] Aunque los mismos no se encuentren amparados por "derecho de admisión" alguno, como hemos tenido ocasión de presentar anteriormente.

[122] En este sentido, cfr. artículo 19 del RDENI, que establece algunas normas a los prestadores de servicios de certificación para que codifiquen adecuadamente los datos de identificación de los firmantes; en especial, reviste importancia la norma que persigue establecer métodos para diferenciar el primer apellido del segundo, lo cual ofrece muestra de la complejidad práctica de esta cuestión.

287 y ss.) sobre el tratamiento de los datos de carácter personal de los certificados, que examinaremos sucintamente.

Con carácter general, el artículo 17.1 de la LFE determina la necesidad de que el prestador de servicios de certificación adecue su actividad a las prescripciones de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal y a su normativa de desarrollo, principalmente el Real Decreto 1720/2007, de 21 de diciembre, imponiéndose la misma obligación a los órganos administrativos en el ejercicio de sus funciones de supervisión y control estatal.

De acuerdo con el artículo 17.2 de la LFE, los prestadores que emitan certificados al público sólo pueden obtener datos directamente de los firmantes (suscriptores de certificados) o bien con su consentimiento previo y expreso.

Los datos a captar serán los necesarios para la emisión y el mantenimiento del certificado electrónico, así como para la prestación de otros servicios en relación con la firma electrónica. Estos datos habitualmente incluyen nombre y apellidos (artículo 11.1.e) de la LFE), documento nacional de identidad (artículo 11.1.e) de la LFE) o equivalente, datos de verificación de firma (artículo 11.1.f) de la LFE), dirección electrónica (para las finalidades de firma y cifrado de correo electrónico, de acuerdo con las especificaciones S/MIME) y datos de contacto (dirección postal, teléfono y otros).

En el procedimiento de captación o recogida de los datos, hay que cumplir las exigencias del artículo 5 de la LOPD. Además, los datos captados para la prestación del servicio de certificación no podrán ser utilizados para ninguna finalidad diferente sin el consentimiento expreso del firmante, prescripción que ya que se encuentra contenida, con carácter general, en el artículo 4 de la LOPD, del cual deriva la necesidad de obtener el consentimiento del afectado, en caso de cambio de finalidad del tratamiento de los datos personales.

Nada dice la Ley sobre el régimen de consentimiento necesario para la captación de los datos personales en entornos cerrados de usuarios (trabajadores y empleadores, clientes y proveedores), en los que no existe prestación al público, dando por supuesto

que los datos ya constan en poder del prestador de servicios de certificación.

En este caso, sin embargo, también hay que aplicar las normas generales de la LOPD, y cuando no sea necesario el consentimiento previo, de acuerdo con los casos que se prevén en los artículos 6 y 11 de la LOPD, será necesario en todo caso informar a los afectados del tratamiento en relación con el certificado electrónico.

De acuerdo con el artículo 17.4 de la LFE, queda prohibido a los prestadores de servicios de certificación incluir en los certificados ningún dato de los indicados en el artículo 7 de la Ley Orgánica 15/1999, incluso con la solicitud previa y el consentimiento del firmante. Estos datos son los siguientes:

- Ideología, religión o creencias.
- Afiliación sindical.
- Raza, salud y vida sexual.
- Infracciones penales o administrativas.

Aún esta prohibición, parece que la posibilidad de emitir certificados a los miembros de un partido político, o de un sindicato, ha de ser admitida, y estos certificados, aunque no informen expresamente de los datos prohibidos, ciertamente de forma implícita suministran esta información a los terceros (cosa, por otra parte, muy razonable y habitual en el mundo físico, en forma de "carné" del partido o del sindicato).

Hasta aquí la regulación legal que, como podemos ver, nada prevé acerca del tratamiento de protección de datos personales en las relaciones entre los terceros receptores de documentos firmados electrónicas y los prestadores de servicios de certificación. La cuestión es que, de acuerdo con la legislación, el prestador debe suministrar informaciones de verificación de estado de certificados a los terceros, lo

cual, en algunos casos, supone la cesión de datos personales[123].

Además, aunque no se dice en la LFE, los terceros destinatarios de documentos firmados también deben proteger adecuadamente los datos personales, y especialmente han de tener en cuenta que la finalidad de los datos certificados que reciben es verificar la firma del suscriptor del certificado, y que por tanto no podrán utilizar estos datos para ninguna otra finalidad, sin el consentimiento expreso del suscriptor[124].

En esta línea, cabe indicar que algunos prestadores de servicios de certificación ya venían estableciendo en sus contratos, de forma habitual, un régimen de uso de los datos personales por parte de los terceros receptores de documentos firmados electrónicamente, si bien no todos lo habían previsto[125].

Seguramente por esta omisión de la LFE en relación con los datos certificados, y también por la total ausencia de regla legal en relación con los datos personales que soporten sistemas de firma electrónica que no empleen certificados, el RDLAE y la LUTICAJ han adoptado estas prevenciones legales.

Y a todo ello, dentro del régimen de uso de la firma electrónica en la Administración electrónica, hay que añadir la obligación de publicar la relación de sistemas de firma electrónica que, conforme a lo previsto en esta Ley, sean admitidos o utilizados en la sede (artículo 15.2 de la LAE y artículo 11.1.d) de la LUTICAJ), previsión orientada claramente a permitir que los usuarios de la sede conozcan los sistemas que efectivamente pueden emplear.

---

[123] En principio, el firmante incluye su certificado dentro de la firma electrónica, de forma que el tercero ya ha obtenido todas las informaciones personales directamente del firmante (así sucede en el caso de los estándares XAdES, CAdES y PAdES), pero existen otros casos en los que la firma no incluye el certificado, sino que éste se entrega por el prestador al tercero, con lo cual se produce la comunicación de datos a la que nos referimos (por ejemplo, en XMLDSig con XKMS).

[124] Consentimiento que, por otra parte, se puede obtener electrónicamente, con la propia firma electrónica.

[125] Es más, desde el momento en que parte de la doctrina considera que no tiene ningún sentido establecer un contrato con los terceros verificadores, resulta más que interesante que exista alguna previsión legal que regule la cuestión. Cfr. ORTEGA DÍAZ: 2008.

2.3 LA VERIFICACIÓN DE LA FIRMA ELECTRÓNICA COMO ACTO ADMINISTRATIVO

La verificación de firma electrónica es un procedimiento mediante el cual un tercero destinatario de un documento firmado puede comprobar la existencia y validez de la firma electrónica y, por lo tanto, de las propiedades de integridad y autenticidad del documento electrónico.

Cabe preguntarse por la naturaleza jurídica de la actuación de verificación de la firma electrónica, y sus elementos asociados, cuando dicha actuación es realizada por la Administración pública receptora de documentos.

A nuestro juicio, se trata de un verdadero acto administrativo de trámite, que podemos caracterizar como singular y de tracto instantáneo, y que produce efectos externos en el procedimiento (GARCÍA DE ENTERRÍA Y FERNÁNDEZ, 2008a: pp. 577 y ss.), en particular en cuanto a la consecuencia de su resultado, típicamente la aceptación o rechazo de un documento electrónico por el registro de entrada.

2.3.1 La carga de verificar la firma electrónica recae sobre la Administración receptora de documentos firmados

En efecto, la Administración se encuentra sujeta a la verificación de la firma electrónica, y del certificado en que se basa, antes de poder confiar en ella, asumiendo, en el caso de sistemas basados en certificados electrónicos, el rol de tercero de buena fe que confía en certificados[126]; esto es, el tercero es toda persona, diferente de un suscriptor de certificados expedidos por un prestador de servicios de certificación, que recibe documentos firmados, con los correspondientes certificados, que debe verificar las firmas y los certificados, antes de poder confiar.

[126] Esta es la situación, al menos, en el caso de la Administración que admite certificados a los ciudadanos o a otras Administraciones, a diferencia de los certificados corporativos expedidos a sus órganos, cargos y empleados públicos por la propia Administración, donde no podría afirmarse con

No se trata, propiamente, de una obligación legal, dado que ni la LFE ni la LAE o la LUTICAJ la instituyen, sino más bien de una carga del destinatario de firmas electrónicas[127], cuya no observancia conlleva aparejada la exoneración de responsabilidad del prestador de servicios de certificación, según dispone el artículo 23.4 de la LFE, que dispone que "el prestador de servicios de certificación tampoco será responsable por los daños y perjuicios ocasionados al firmante o a terceros de buena fe si el destinatario de los documentos firmados electrónicamente actúa de forma negligente.

Se entenderá, en particular, que el destinatario actúa de forma negligente en los siguientes casos:

a) Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

b) Cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica".

Como se puede ver, dos son los contenidos mínimos de la diligencia que deberá observar la Administración cuando actúe como tercero de buena fe: la aplicación de los límites materiales y cuantitativos de uso del certificado, y la comprobación del estado del certificado, para determinar si el mismo se encontraba vigente en el momento de la firma electrónica; sin perjuicio de otros elementos de diligencia no determinado en el texto legal.

Como veremos al referirnos a los dispositivos de verificación de firma[128], el artículo 25.3 de la LFE determina que el procedimiento de verificación debe garantizar,

---

tanta facilidad su condición de tercero.

[127] VALERO TORRIJOS, 2008: p. 47, ha notado que de la no verificación de la firma electrónica no se desprendería, en puridad, la invalidez del documento, situando el problema en el plano de la eficacia, postura que, en nuestra opinión, es absolutamente correcta.

[128] Cfr. sección 5.3.2 de este trabajo.

siempre que sea técnicamente posible, los siguientes aspectos[129]:

- Los datos utilizados para verificar la firma deben corresponder con los datos mostrados a la persona que verifica la firma.

- La firma se debe verificar con fiabilidad y el resultado de la verificación se debe presentar correctamente.

- La persona que verifica la firma electrónica debe poder, si es necesario, establecer con fiabilidad el contenido de los datos firmados y detectar si han sido modificados.

- Se deben mostrar correctamente tanto la identificación del firmante o, en su caso, constar claramente la utilización de un seudónimo, como el resultado de la verificación[130].

- Se deben verificar de manera fiable la autenticidad y la validez del certificado electrónico correspondiente.

- Se debe poder detectar cualquier cambio relativo a su seguridad[131].

Como tendremos ocasión de estudiar *infra*[132] con detalle, la política de firma electrónica y de certificados de la Administración establece, en gran medida, los contenidos del procedimiento de verificación de firma electrónica, condicionando incluso la actuación del suscriptor del certificado cuando procede a la creación de la firma electrónica.

Por ello, resta sólo por decir, en este momento, que a nuestro juicio se trata de un acto

[129] Resulta criticable, en nuestra opinión, que el texto legal parezca considerar que siempre será una persona física quien proceda a la verificación manual de la firma electrónica, en particular por la posibilidad de realizar esta actuación de forma automatizada.

[130] Requisito que es redundante con el segundo requisito del artículo 25.3 de la LFE.

[131] Es de suponer que hace referencia a la firma electrónica verificada.

[132] Cfr. la sección 4.3 de este trabajo.

administrativo automatizable[133], y precisamente en atención a la existencia de una política de firma dictada al amparo de la regulación vigente se puede evaluar el cumplimiento de las condiciones de adecuada programación que, al efecto, exige el artículo 39 de la LAE.

2.3.2 ¿Está obligada la Administración a cumplir las condiciones generales de verificación predispuestas por los prestadores de servicios de certificación?

Pese a la existencia del artículo 25.3 de la LFE al que nos acabamos de referir, el procedimiento de verificación de firma electrónica – y del resto de los elementos que le dan soporte, como los certificados – es uno de los más descuidados en la regulación, por lo que se ha podido observar el intento de determinar convencionalmente el modelo de verificación, la diligencia exigible y los efectos de la verificación, en otra muestra del fenómeno de la autorregulación.

En efecto, y sobre todo desde la perspectiva de los prestadores de servicios de certificación, se pretende regular la verificación de firmas y certificados mediante las condiciones generales de uso de los certificados, que contienen una descripción pormenorizada de los requisitos y de la ejecución del procedimiento y, supuestamente, obligan a los terceros que confían en certificados: ¿cabe entender a la Administración sujeta a estas condiciones?

Por ejemplo, las condiciones generales de uso de los certificados idCAT[134] emitidos por la Agencia Catalana de Certificación determinan los requisitos siguientes y la verificación correspondiente, que deben cumplir cualesquiera personas que hagan uso

[133] Quizá no resulte aventurado decir que la verificación de la firma electrónica es el acto administrativo automatizado más extendido en la práctica, si bien no se percibe como un acto diferente del trámite de "registrar de entrada", igualmente automatizable.

[134] Las citadas condiciones generales de uso se incorporan por referencia a los certificados, en un campo concreto del certificado, que apunta a la dirección de la página web del prestador de servicios, en la cual se publica el texto de las mismas.

de los citados certificados: "Para confiar en un mensaje o documento, el verificador debe validar dos firmas:

- En primer lugar, debe verificar la firma electrónica del mensaje o documento. Esta comprobación es imprescindible para determinar que fue generada por el suscriptor, utilizando la clave privada correspondiente a la clave pública contenida en el certificado idCAT, y para garantizar que el mensaje o documento firmado no fue modificado desde la generación de la firma electrónica.

- En segundo lugar, debe verificar la firma electrónica del certificado idCAT del suscriptor. Esta comprobación es imprescindible para determinar que la clave pública contenida en el certificado idCAT corresponde al suscriptor.

  La comprobación será ejecutada normalmente de manera automática por el software del verificador y, en todo caso, debe serlo de acuerdo con la declaración de prácticas de certificación, con los siguientes requisitos:

- Hay que utilizar el software apropiado para la verificación de una firma digital con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma electrónica a verificar, ya que para verificarla se utiliza esta cadena de certificados.

- Hay que asegurar que la cadena de certificados empieza con la entidad de certificación EC-ACC, que es la más adecuada para la firma electrónica del certificado idCAT que se verifica, ya que una firma electrónica puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse de utilizar la cadena más conveniente para verificarla.

- Hay que comprobar el estado de revocación de los certificados de la cadena con la información suministrada en el Registro de certificación de CATCert (con LRCs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que sólo puede considerarse correctamente

verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.

- Hay que verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el firmante.

- Hay que determinar la fecha y hora de generación de la firma electrónica, ya que la firma electrónica sólo puede considerarse correctamente verificada si se creó dentro del período de vigencia de la cadena de certificados en que se basa.

- Hay que delimitar los datos firmados digitalmente que se utilizarán en la validación de la firma.

- Finalmente, hay que verificar técnicamente la propia firma con el certificado del firmante avalado por la cadena de certificados".

En primer lugar, hay que indicar que la doctrina ha criticado la posible consideración de estas condiciones como verdaderas cláusulas contractuales, indicando que los terceros receptores de mensajes firmados no tienen una relación contractual con el prestador de servicios que expidió el certificado.

ORTEGA DÍAZ, 2008: pp. 255 y ss., ha indicado que el contrato de certificado digital que regula la relación entre el prestador y el firmante, debe contener necesariamente una estipulación en favor de tercero, en virtud de la cual el prestador deberá conceder acceso a dicho tercero al certificado y a la información de estado de vigencia. De este modo, “el tercero, cuando acude al prestador de servicios de certificación para obtener la copia del certificado y la de su clave pública asociada – con el fin de verificar tanto la firma como el estado de vigencia del certificado electrónico –, está exigiendo al certificador el cumplimiento del derecho de crédito que a su favor se deriva del contrato de certificación. Vemos, así, cómo entre las partes contractuales – certificador y usuario (suscriptor) – existe una relación contractual y entre una de las partes, el certificador, y el tercero, una relación obligatoria”, de la que el autor citado deduce la posibilidad de que el tercero usuario de certificados pueda exigir

responsabilidad contractual al prestador que le cause un daño[135].

Aun adoptando esta posición, lo cierto es que el prestador de servicios de certificación, como hemos visto, se puede exonerar de responsabilidad "si el destinatario de los documentos firmados electrónicamente actúa de forma negligente", y hemos confirmado que el tercero receptor de documentos firmados, en este caso la Administración, aun no siendo parte de un contrato con el prestador, tiene una relación obligacional con el prestador, pudiendo entenderse legítimo que la misma sea modulada por el contrato entre el suscriptor del certificado y el prestador.

Esto es, si en el contrato entre el prestador del servicio y el ciudadano (suscriptor del certificado) las partes pactan las condiciones que deberán cumplir los terceros receptores de los documentos firmados para que su confianza en la firma electrónica sea aceptable, no parece que resulte objetable trasladar estas condiciones a los terceros[136], por vía de estas condiciones generales de uso de certificados o empleando la Declaración de Prácticas de Certificación.

Refuerza este argumento que el articulo 18.b) de la LFE obligue a todo prestador de servicios de certificación a informar a los solicitantes de certificados de una serie de aspectos relevantes, incluyendo los posibles dispositivos de verificación de firma compatibles, los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo o las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial; indicándose que "la información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos", lo cual implica que deberán ser mínimamente diligentes en el uso del certificado.

---

[135] ORTEGA DÍAZ, 2008: p. 345. Nótese que se diferencia a estos terceros verificadores de otros terceros "puros", que en caso de sufrir daños por la actividad del prestador podrán acudir a la vía de la responsabilidad extracontractual. Cfr. en el mismo sentido, PÉREZ PEREIRA, 2009: p. 204.

[136] Caso discutible sería la aparición, en dichas condiciones generales, de exoneraciones totales de responsabilidad, o de obligaciones desproporcionadas para el tercero, o de imposible cumplimiento, que entendemos afectarían al objeto esencial del contrato de certificación.

Por lo cual cabe entender que, con carácter general, la Administración deberá cumplir con la diligencia prevista en dichas condiciones generales, o asumir el riesgo de asumir la exoneración de responsabilidad del prestador, por su actuación negligente.

En el procedimiento de verificación de firma electrónica que estamos analizando tiene un papel protagonista indudable la política de firma electrónica, dado que, en gran medida, determina precisamente las reglas que aplica la Administración en la verificación de la firma electrónica[137], de forma que, en nuestra opinión, en el diseño de la citada política se deberán considerar las condiciones generales de uso de los certificados admitidos.

2.3.3 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, en nuestra opinión, 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[138], 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

[137] Cfr. la sección 4.3.1.4 de este trabajo.

[138] Actualmente hay veinte prestadores que han comunicado al supervisor la expedición de certificados reconocidos; a los que hay que añadir a los prestadores del resto de Estados de la Unión Europea que expiden certificados reconocidos, que gozan de reconocimiento directo, mediante la consulta de la lista de servicios de confianza (TSL) publicada por todos los Estados de la Unión.

a cada Administración competente, que deberá aportar el servicio de validación.

No podemos estar de acuerdo con la posibilidad de centralizar este servicio en la Dirección General de la Policía, como se ha propuesto para el ámbito de la Administración electrónica[139]; entre otros motivos, porque dicho órgano ni siquiera aloja los servicios de verificación del DNI electrónico en orden a evitar sospechas infundadas de excesivo conocimiento por el Estado de los usos que hacen los usuarios de este sistema de firma[140].

De hecho, un tal modelo podría ser considerado como un peligro potencial importante a la privacidad (Cfr. VALERO TORRIJOS y SÁNCHEZ MARTÍNEZ, 2007), argumento que en general parece desaconsejar la existencia de una única plataforma de verificación.

Acertadamente, merece especial prudencia para VALERO TORRIJOS, 2009: pp. 194, la consideración del impacto que para la protección de datos puede suponer la combinación entre el DNI electrónico, por su relevancia y singularidad, y la información de revocación necesaria para la validación, especialmente en que caso de que el mismo prestador ofrezca el servicio de certificación y el de verificación.

A su juicio, "teniendo en cuenta que el sistema de identificadores electrónicos único exige que todos los ciudadanos dispongan de un certificado expedido por un mismo prestador de servicios, resultan evidentes los enormes riesgos que, en materia de privacidad, tal medida organizativa conlleva por cuanto, a menos que se estructuren de forma separada la base de datos propia de los certificados y la relativa a los que se encuentran revocados y se garantice adicionalmente que no se archiven las consultas realizadas en ésta última, un eventual problema de seguridad permitiría confeccionar un completísimo perfil de lo ciudadanos por lo que se refiere a sus actividades telemáticas en las que utilicen este sistema de identificación electrónica".

---

[139] Cfr. MARTÍNEZ GUTIÉRREZ, 2009: p. 573., si bien el mismo autor ha matizado su posición posteriormente, apostando por @firma, sin perjuicio de la existencia de otras plataformas de validación integradas en el sistema nacional de verificación de certificados. MARTÍNEZ GUTIÉRREZ, 2011: pp. 442 y ss.

[140] No ya digamos de los certificados de terceros prestadores. Además, del hecho de que el DNI-e aspire a ser instrumento de identificación y firma electrónica universal no se deriva ninguna idoneidad del emisor del DNI-e para verificar el estado de los restantes certificados, expedidos por otras entidades.

Si bien continúa el autor diciendo que la regulación de la Dirección General de la Policía no aclara si existen medidas preventivas que mitiguen este riesgo, lo cierto que 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[141].

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.

Y por lo que se refiere a la singularidad del DNI electrónico anteriormente aludida, como se puede verificar en la página web institucional del DNI electrónico[142], "en la Infraestructura de Clave Pública adoptada para el DNI electrónico, se ha optado por asignar las funciones de Autoridad de Validación a entidades diferentes de la Autoridad de Certificación, a fin de aislar la comprobación de la vigencia de un certificado electrónico de los datos de identidad de su titular.

Así, la Autoridad de Certificación (Ministerio del Interior – Dirección General de la Policía) no tiene en modo alguno acceso a los datos de las transacciones que se realicen con los certificados que ella emite y las Autoridades de Validación no tiene acceso a la identidad de los titulares de los certificados electrónico que maneja, reforzando – aún más si cabe – la transparencia del sistema".

En otro orden de cosas, el RDENI ha regulado, en su artículo 20, el conjunto mínimo de requisitos aplicables a las plataformas de validación de certificados y firmas

[141] Las plataformas del Ministerio de Hacienda y Administraciones Públicas, del IZENPE vasco o de la Agència Catalana de Certificació (CATCert), entre otros servicios, suponen ejemplos de prestación de estos servicios.

[142] http://www.dnielectronico.es/Autoridades_de_Validacion/index.html (última visita: 29/07/2012). Esta información también se encuentra refrendada en la Declaración de Prácticas de Certificación de la Policía. Cfr. secciones 1.3.4, 4.9.7, 4.9.9, 4.9.10 y 4.10.

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[143].

- 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[144] 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

[143] Como se puede ver, el ámbito es muy superior al previsto en el artículo 21 de la LAECSP, que se limita a la verificación del estado de vigencia de los certificados.

[144] Sólo dentro del contexto de una norma reglamentaria que establezca condiciones adicionales al uso de la firma electrónica parece posible obligar a los prestadores de servicios de certificación a adoptar prácticas específicas en su negocio, que como sabemos, se encuentra sujeto a libre concurrencia. Alternativamente, se podría acudir a la creación de un sistema voluntario de certificación de la actividad

interoperables entre las distintas Administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza (TSL)[145].

de los prestadores (cfr. artículo 26 de la LFE).

[145] Si bien hay que recordar que dicho sistema ha sido diseñado y aprobado en relación con la ventanilla única administrativa, lo cual puede generar algunos conflictos (irónicamente, de interoperabilidad legal) en su aplicación a otros usos de Administración electrónica.

3 "HAGAN USTEDES LAS LEYES…": LA POLÍTICA DE FIRMA ELECTRÓNICA Y CERTIFICADOS

Como en la célebre cita atribuida a D. Álvaro de Figueroa y Torres, primer Conde de Romanones, veremos a partir de este capítulo el verdadero régimen de admisión y uso de la firma electrónica que, por supuesto, se encuentra en el reglamento.

De hecho, en varios reglamentos, incluyendo el RDENI, el RDENS, el RDLAE, y su desarrollo, en particular las Normas Técnicas de Interoperabilidad. Todo un ejercicio de virtuosismo reglamentista cuyo efecto práctico limita y condiciona los derechos instituidos en la legislación, y no poco, y que cabe cuestionar se justifique realmente en la necesidad de interoperabilidad.

Por ello, en este capítulo presentamos, desde una perspectiva jurídica, las políticas de firma electrónica y de certificados, a partir del análisis de su necesidad como elemento regulador, su conceptualización normativa y su naturaleza jurídica; así como los principales problemas que plantean los contenidos de la regulación.

3.1 INTRODUCCIÓN Y NECESIDAD DE UNA POLÍTICA DE FIRMA ELECTRÓNICA Y CERTIFICADOS

A lo largo de los pasados años hemos tenido la oportunidad de asistir a un interesante debate doctrinal alrededor de la firma electrónica, que en la mayoría de los casos se ha centrado en las condiciones de calidad y seguridad necesarias para la emisión de los certificados electrónicos X.509 v3 en los que habitualmente se fundamenta la firma, y que se formalizan en la denominada "política de certificación" así como en la legalmente exigible[146] "declaración de prácticas de certificación".

Sin embargo, en pocas ocasiones se ha abordado un tema de importancia capital para el funcionamiento de la firma electrónica, como es el de la gestión del ciclo de vida de

[146] Cfr. artículo 19 de la LFE, que establece los contenidos mínimos de esta declaración obligatoria que

la firma electrónica y, en conexión, ciertas normas aplicables a los certificados electrónicos disponibles en el mercado[147].

En primer lugar, hay que constatar que no sólo existe una notable diversidad en materia de certificados digitales, sino que también nos encontramos inmersos en un sistema donde coexisten diferentes tecnologías relacionadas con la firma, que por supuesto inciden de forma absolutamente decisiva en el uso y la gestión posterior de la firma electrónica, de entre las que merece la pena al menos citar las siguientes:

- Existen al menos dos grandes formas de estructurar y codificar la firma electrónica, con implicaciones importantes en la sintaxis de la firma electrónica[148].

- Por otra parte, los sistemas empleados para la validación de los certificados son cada vez más variados. En primer lugar, existen diferentes formas de organizar la Infraestructura de certificación de clave pública (PKI), que deben ser soportadas por los mecanismos de validación para poder comprobar la corrección de los certificados que avalan la firma[149]. En segundo lugar, existen diferentes prácticas y mecanismos para proceder a la comprobación de los certificados[150].

- También merece la pena mencionar la existencia de diferentes mecanismos

---

deben realizar los prestadores de servicios de certificación.

[147] Para una descripción de los principales tipos de certificados, cfr. capítulo 6.1 de este trabajo.

[148] Por una parte tenemos PKCS#7 y su evolución posterior en el IETF, conocido como CMS – Cryptographic message syntax (sintaxis de mensaje criptográfico), y que emplea la notación de sintaxis abstracta número 1 (ASN.1) definida por la Unión Internacional de Telecomunicaciones en su especificación X.280. Por otra parte, ha irrumpido con fuerza la noción de estructura de firma electrónica en XML, principalmente fomentada por los foros técnicos W3C y OASIS. Las especificaciones del ETSI se han escrito en los dos formatos. Respecto a la codificación, en ASN.1 se emplea DER y en XML, base64. Cfr. la sección 3.4 de este trabajo.

[149] La PKI jerárquica, la certificación cruzada, las listas de Autoridades de certificación (incluyendo listas blancas, negras, grises, con y sin puntuación de seguridad), o las Autoridades de certificación puente son sólo algunas de las posibilidades propuestas.

[150] Incluyendo las listas de revocación de certificados, el protocolo en línea de comprobación de estado de certificados (OCSP), el protocolo sencillo de validación de certificados (SCVP), el esquema de gestión de claves en XML (XKMS) y otros que emergen.

para indicar cualidades o propiedades, llamadas atributos, como la pertenencia a una organización, el cargo, los poderes y las autorizaciones, incluyendo los llamados certificados de atributos, entre otras soluciones, sin que existan formas de tratamiento normalizado.

- Finalmente, resulta necesario definir cuestiones muy importantes en el ciclo de vida de la firma electrónica con elementos complejos, como el sello de tiempo o los atributos a verificar durante la generación de la firma, o referente al mantenimiento del período de validez de la firma electrónica a lo largo de los años en que la documentación se encuentra activa, o a su posterior archivo definitivo.

En segundo lugar, a medida que se empieza a emplear la firma digital para diferentes aplicaciones, se hace cada vez más necesario definir el significado y las consecuencias concretas de esta firma digital, que en algunos casos va a representar un acto de voluntad de una persona, mientras que en otros casos sencillamente va a proteger el documento original en soporte informático como si en soporte papel el documento fuese plastificado.

Los diferentes usos de la firma electrónica deben plasmarse en la propia firma generada si en el futuro necesitamos leer una firma electrónica y entender con claridad cuál era su fundamento y objetivo y, por tanto, las garantías ofrecidas por la misma.

Los elementos principales que hemos visto hasta este momento – la existencia de múltiples certificados, la proliferación de formatos, procedimientos y métodos de firma y de validación de la misma, y la problemática del significado y garantías de la firma – hacen notar la necesidad de gestionar adecuadamente las firmas electrónicas.

Para ello, y bajo los auspicios del grupo Iniciativa Europea de Normalización de la Firma Electrónica – una muestra bastante clara de la tecnocracia y expertocracia organizada a las que se refiere ESTEVE PARDO, 2010, pp. 235 y ss. – impulsado por la Comisión Europea y la industria, el Instituto Europeo de Normas de Telecomunicaciones (en adelante, el "ETSI") ha producido diversas especificaciones técnicas voluntarias que

tratan la gestión de las firmas electrónicas mediante políticas de seguridad especialmente diseñadas al respecto, denominadas "políticas de firma electrónica".

En concreto, resulta imprescindible referirse a las siguientes:

- ETSI TS 101 733 v1.8.1 (2009-11). Firmas electrónicas avanzadas CMS (CAdES). En este documento se especifica la sintaxis de las firmas electrónicas en ASN.1[151], dentro de la cual se describe cómo referenciar una política de firma electrónica, de forma que el destinatario de un documento firmado sepa qué política de firma se debe aplicar para la verificación de la firma.

- ETSI TS 101 903 v1.4.1 (2009-06). Firmas electrónicas avanzadas XML (XAdES). En este documento se especifica la sintaxis de las firmas electrónicas en XML[152], dentro de la cual se describe cómo referenciar una política de firma electrónica, de forma que el destinatario de un documento firmado sepa qué política de firma se debe aplicar para la verificación de la firma.

- ETSI TR 102 272 v1.1.1 (2003-12). Formato ASN.1 para políticas de firma. En este documento se especifica la sintaxis para la representación de una política de firma electrónica en ASN.1.

- ETSI TR 102 038 v1.1.1 (2002-04). Formato XML para políticas de firma. En este documento se especifica la sintaxis para la representación de una política de firma electrónica en XML.

- ETSI TR 102 041 v1.1.1 (2002-02). Informe sobre políticas de firma electrónica.

- ETSI TR 102 045 v1.1.1 (2003-03). Política de firma para modelo de negocio ampliado.

Una política de firma electrónica puede conceptuarse como un conjunto de reglas que se emplean en la creación y en la validación de una firma electrónica, de acuerdo con

[151] Algunas aplicaciones de uso común que utilizan esta sintaxis son Adobe PDF o el correo electrónico seguro S/MIME (implantado en Mozilla Thunderbird o Microsoft Outlook).

[152] Algunas aplicaciones de uso común que utilizan esta sintaxis son OpenOffice o Microsoft Office 2010.

las cuales se puede considerar que una firma electrónica es válida.

Un contexto legal o contractual puede reconocer una determinada política de firma como elemento bastante para cumplir los requisitos que exige para cierto acto, como sucede en el comercio electrónico[153] o en el procedimiento administrativo por vías telemáticas.

Por ejemplo, una persona u organización puede establecer una política de firma para determinar los elementos que exige a una firma antes de confiar en ella, como puede ser el empleo de cierto tipo de certificado, el significado del acto de firma, los algoritmos que se emplearán para la firma y su verificación, el uso de sellos de tiempo y otras condiciones. El firmante podría escoger el empleo de esta política de firma antes de firmar, para indicar su conformidad con la misma, eliminando algunas de las incertidumbres que pueden existir en el escenario telemático donde se va a emplear la firma electrónica.

Se trata de lograr que el firmante y el verificador empleen la misma política de firma, y que esta política de firma regule las condiciones en las que las partes confían en una firma para un contexto de seguridad dado[154].

La política de firma puede ser identificada de forma explícita por la semántica de los datos firmados o por un dato externo a los datos firmados, como por ejemplo un contrato o una norma administrativa, que incluye por referencia una política de firma:

- Cuando existe un contrato que sustenta la validez de la firma electrónica, hablamos de firma electrónica convencional[155].

---

[153] HERNÁNDEZ ARDIETA *et al*, 2008, pp. 309 y ss, presentan un interesante ejemplo práctico de aplicación de las políticas de firma electrónica para transacciones comerciales.

[154] En este sentido, la Guía de aplicación de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados (MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA, 2011: p.15) indica que "la finalidad de una política de firma electrónica es por tanto reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado. Este contexto puede ser una transacción determinada, un régimen legal, un rol que asuma la parte firmante o cualquier otro ámbito".

[155] Recuérdese que el artículo 3.10 de la LFE establece que "a los efectos de lo dispuesto en este

- Cuando la validez viene dada por una norma administrativa, entonces hablamos de firma electrónica normativa.

Definiendo políticas de firma electrónica se completan las carencias legales, mediante una autorregulación técnico-jurídica, que permite implantar un modelo de gestión flexible y realista.

3.2 EL CONCEPTO JURÍDICO DE POLÍTICA DE FIRMA ELECTRÓNICA Y CERTIFICADOS

Una vez introducida y justificada la necesidad de disponer de una política de firma electrónica, procede analizar la conceptualización jurídica que de la misma se realiza en el ámbito de la Administración electrónica.

Veremos, en primer lugar, las definiciones iniciales del concepto, que se han producido en la Administración General del Estado; la definición general del Esquema Nacional de Interoperabilidad y, finalmente, el concepto de política marco de firma electrónica y de certificados.

3.2.1 Las definiciones iniciales en la Administración General del Estado

La primera referencia[156] normativa al concepto de política de firma electrónica se encuentra en la Orden PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre

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".

[156] Las referencia técnicas al concepto de política de firma electrónica resultan anteriores, como se puede ver en ALAMILLO DOMINGO, 2000, y 2003, pp. 68 a 72.

particulares.

En esta Orden se establecen unos estándares y condiciones técnicas uniformes en la emisión y remisión de facturas que afecten a la Administración General del Estado y a los organismos públicos vinculados o dependientes de la misma. Entre las condiciones aplicables a las facturas electrónicas, se indica que las mismas deberán hallarse en el formato que se determina en el anexo de esta orden, ajustándose el formato de firma electrónica a la especificación XML-Advanced Electronic Signatures (XAdES), ETSI TS 101 903, incluyendo el documento de la política de firma[157].

Sin embargo, la primera referencia normativa de corte general a la política de firma electrónica, aunque resulta aplicable sólo en el ámbito de la Administración General del Estado, se encuentra en el artículo 24.1 del RDLAE, con el siguiente tenor: "La política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación."

Se trata de una definición de corte muy genérico, que se refiere, de forma muy amplia, a directrices y normas técnicas para el uso de los sistemas de firma electrónica, y que se completa con la caracterización de los contenidos mínimos de la misma debe tener, que incluyen:

"a) Los requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y de sus organismos públicos.

b) Las especificaciones técnicas y operativas para la definición y prestación de los servicios de certificación asociados a las nuevas formas de identificación y autenticación de la Administración General del Estado recogidas en el presente real

[157] De acuerdo con el anexo de la Orden ministerial, dicho documento de política de firma, que debe seguir el formato «Facturae», para su uso con alguna Administración Pública del ámbito de la presente orden, se encuentra igualmente disponible en la página Web www.facturae.es bajo el enlace «Política de Firma Formato Facturae». En tal documento se recoge el formato que debe seguir este elemento. Esta política de firma se adaptará a la que establezca la Administración General del Estado.

decreto.

c) La definición de su ámbito de aplicación".

3.2.2 La definición y el contenido de la política de firma electrónica y de certificados en el ENI

La segunda, y más importante, definición de política de firma electrónica y de certificados de la Administración se encuentra en el anexo del RDENI, y corresponde al "conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma".

A diferencia de la definición del RDLAE, en este caso – y con alcance general, por la condición de norma básica del RDENI, sí se identifica qué sea una política de firma electrónica, en el sentido de ordenar un conjunto de medidas a una finalidad, que no es otra que regular el ciclo de vida de la firma electrónica, desde su generación hasta su eliminación, garantizando su función administrativa y efectividad jurídica.

El Instituto Europeo de Normas de Telecomunicaciones[158] se refiere a la política de firma electrónica como un conjunto de reglas que define los requisitos técnicos y procedimentales para la creación y la verificación de una firma electrónica, con la finalidad de cumplir una necesidad particular de negocio, y de acuerdo con la cual se puede determinar la validez de la firma electrónica (Cfr. ETSI, 2002a: p. 7, 2002b: p. 8, 2003b: p. 8, 2009b: p. 13).

Esta definición, anterior en el tiempo a la que se incluye en el RDENI, enfatiza la finalidad de la política de firma electrónica, que se entiende como un acuerdo de tipo técnico entre firmante y verificador para lograr un procesamiento consistente de la

[158] El grupo de trabajo ESI – Electronic Signatures Infrastructures, perteneciente al Comité Técnico de Seguridad (TC SEC) es el que desarrolló el concepto de política de firma electrónica que hoy ha adoptado la normativa española.

firma electrónica en un contexto concreto de transacción[159].

Hay que notar, en cualquier caso, que en el concepto legal de política de firma electrónica y de certificados se establecen las siguientes categorías de reglas:

- Normas de seguridad: La firma electrónica se percibe como un elemento que aporta seguridad a los documentos electrónicos, por lo que resulta preciso establecer previsiones que garanticen esta seguridad, como por ejemplo, el empleo de algoritmos fiables, en detrimento de otros que ya no lo sean.

  Por otra parte, no hay que olvidar que la política de firma electrónica y de certificados forma parte de la familia de las políticas de seguridad de la información[160], hoy reguladas en el RDENS y certificables mediante UNE-ISO/IEC 27001:2007[161].

- Normas de organización: La firma electrónica, para su adecuado funcionamiento en las relaciones electrónicas, exige la definición de roles, funciones y responsabilidades, tanto en cuanto a firmante y verificador, cuanto a terceros que intervienen en los procedimientos correspondientes.

- Normas técnicas: La firma electrónica requiere, obviamente, de la determinación de previsiones de corte tecnológico para su adecuado funcionamiento, en especial a tenor de la ya mencionada diversidad tecnológica, que impide la interoperabilidad, debido a la imposibilidad práctica de que todos los receptores de documentos o mensajes firmados dispongan de todas las posibles tecnologías empleadas para su generación.

  Se aprecia aquí la función de la interoperabilidad como reducción de las

[159] En este sentido, resulta de gran importancia establecer el contexto de la política de firma electrónica, incluyendo los elementos de la transacción (ETSI, 2002a: p. 8 y ss.)

[160] Con mucha seguridad, este instrumento se denomina precisamente "política" por haber sido considerada una especial política de seguridad, aplicable a la firma electrónica.

[161] La norma UNE-ISO/IEC 27002:2009 prevé, en sus secciones 10.8.4.d), 10.9.1.b), 10.9.2.a) y f), 10.9.3, 12.3.1, 12.3.2 y 15.1.3, controles referidos a la aplicación de la firma electrónica a la seguridad del negocio conducido electrónicamente.

amplias posibilidades que ofrece la tecnología a un mínimo común, en forma de "perfiles de interoperabilidad"[162], que a partir de los estándares seleccionan un conjunto de opciones técnicas que firmante y verificador se comprometen a adoptar[163].

- Normas legales: La firma electrónica responde a un contexto jurídico concreto, y debe ser diseñada de forma que garantice la validez[164] y, más importante aún, la eficacia del documento o mensaje firmado electrónicamente[165], resultando particularmente importante en este caso el mantenimiento del valor probatorio de la firma electrónica.

Las anteriores categorías se concretan cuando el RDENI indica que la política de firma electrónica y de certificados tratará, entre otras cuestiones recogidas en su definición[166], aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones públicas.

Estas reglas se concretan mediante una Norma Técnica de Interoperabilidad[167], específica para la firma electrónica y los certificados en que ésta se basa, que "tratará,

---

[162] Este concepto de "perfil de interoperabilidad" se emplea de forma habitual en grupos internacionales dedicados a la interoperabilidad, en especial en el ámbito de los servicios web, como por ejemplo la Web Services Interoperability Organization, hoy parte de OASIS (http://ws-i.org/default.aspx, última visita: 30/06/2012).

[163] Dicha técnica también reduce los riesgos y los costes de adopción de la tecnología correspondiente, motivo por el que la interoperabilidad cubre el espacio que existe entre las normas técnicas maduras y la innovación tecnológica.

[164] El cumplimiento de las condiciones exigidas en la LFE permite sustentar la validez de la firma electrónica, en sus diferentes niveles, según hemos visto en la sección 1.3.1 *supra*.

[165] Para lo cual se deben considerar los requisitos de seguridad y proporcionalidad, que llaman al establecimiento de condiciones adicionales al uso de la firma electrónica previstas en la LFE.

[166] Lo cual denota la aproximación de mínimos que informa la Norma Técnica de Interoperabilidad.

[167] Como se puede ver, este conjunto de medidas es de índole diversa, y supera estrictamente la firma electrónica, puesto que alcanzan también a los certificados electrónicos empleados para firmar y a otros

entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones públicas".

La Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados en cuestión ha sido dictada mediante Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública en desarrollo del RDENI (BOE núm. 182 de 30/07/2011), tras su elaboración por el cauce previsto en el artículo 42 de la LAE, y adopta la misma definición[168] que el RDENI, si bien el análisis del objeto de la citada Norma Técnica de Interoperabilidad sitúa la política de firma al servicio del objetivo final de "facilitar el uso de firmas electrónicas seguras e interoperables entres las distintas organizaciones de la Administración Pública", según dispone su apartado I.1.2).

La Guía de aplicación de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados, 2011: pp. 6 y ss., recuerda que la Norma Técnica citada "establece el conjunto de criterios para el desarrollo o adopción de políticas de firma electrónica por parte de las Administraciones públicas", creando un referencial común para que todas las firmas electrónicas generadas bajo una política de firma electrónica aprobada por una Administración pública sean verificables por las restantes[169].

Asimismo, la Norma Técnica de Interoperabilidad "define el contenido de una política de firma electrónica basada en certificados, especificando las características de las reglas comunes, como formatos, uso de algoritmos, creación y validación de firma para

---

elementos accesorios, precisos para la correcta gestión del ciclo de vida de la firma electrónica.

[168] Cfr. apartado II.1.1 de la Norma Técnica de Interoperabilidad.

[169] A esta condición, como veremos, se liga el efecto jurídico de "reconocimiento" (*rectius*, "admisión" efectiva) de la firma electrónica.

documentos electrónicos, así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas", contenidos que se pueden reconducir a tres políticas diferenciadas (Cfr. CROBIES, 2010: p. 7), que colectivamente conforman la política de firma electrónica y de certificados: la política de creación de firma electrónica, la política de validación de firma electrónica y la política de mantenimiento de la longevidad de la firma electrónica.

El epígrafe II.4 de la Norma Técnica de Interoperabilidad, de hecho, concreta la muy importante regla de usos de la firma electrónica, indicando que "las políticas de firma electrónica podrán definir condiciones para la aplicación de una firma electrónica basada en certificados con los siguientes propósitos:

a) Firma de transmisiones de datos, como herramienta para proporcionar seguridad al intercambio, garantizando la autenticación de los actores involucrados en el proceso, la integridad del contenido del mensaje de datos enviado y el no repudio de los mensajes en una comunicación telemática.

b) Firma de contenido como herramienta para garantizar la autenticidad, integridad y no repudio de aquel, con independencia de que forme parte de una transmisión de datos."

Como se puede ver, se prevén dos grandes casos de uso diferenciados: el primero de ellos, más propio de la práctica de seguridad técnica; mientras que el segundo se refiere a los contenidos, es decir, los documentos y mensajes autorizados con firma electrónica.

Adicionalmente, la Norma Técnica de Interoperabilidad "define el contenido de una política de firma electrónica basada en certificados", restringiendo el concepto de política de firma electrónica únicamente a las que se basan en certificados electrónicos.

Este aspecto resulta ciertamente criticable, por cuanto el RDENI no contiene restricción explícita alguna a la posibilidad de una política de firma electrónica

ordinaria[170], o a una política de firma electrónica avanzada que se base en mecanismos diferentes a los certificados electrónicos[171].

Sin embargo, no es menos cierto que las especificaciones técnicas de referencia publicadas por el Instituto Europeo de Normas de Telecomunicaciones se han centrado únicamente en las firmas electrónicas avanzadas basadas en certificados electrónicos, y que por tanto no disponemos de una pauta normalizada para la definición de estas políticas ampliadas a otros tipos de firma electrónica.

En atención a esta situación, parece razonable restringir el tratamiento de la política de firma electrónica de contenidos[172] a los mecanismos que disfrutan del derecho de admisión, para los cuales sí debe estar garantizada la interoperabilidad, avanzando en este punto el dato de que la aprobación de la política de firma electrónica y de certificados por cada Administración es una verdadera obligación jurídica, según dispone el artículo 18.2 del RDENI en términos imperativos[173].

[170] Como hemos tenido ocasión de presentar *supra*, la LAE y la LUTICAJ permiten la provisión y admisión (discrecional) de sistemas de firma electrónica basados en clave concertada de ciudadano, así como la actuación administrativa mediante Código Seguro de Verificación.

[171] Por ejemplo, mediante la generación de firmas electrónicas XMLDSig o CMS con claves RSA previamente intercambiadas (PGP) o almacenadas en depósitos de claves consultables (XKMS).

[172] No parece tan razonable, sin embargo, en relación con las firmas de transmisiones de datos, aunque el hecho de que la política sólo se refiera a mecanismos basados en certificados no prohíbe el empleo de otros sistemas de seguridad técnica (por ejemplo, los servicios web de transmisiones de datos se pueden asegurar con firmas digitales basadas en certificados o en claves previamente intercambiadas). Además, se hubiesen podido prever, para estos casos, normas adicionales en cuanto al uso de certificados excluidos de la LFE, como los certificados de dispositivo seguro (diferentes de sello electrónico).

[173] Así, "las Administraciones públicas aprobarán y publicarán su política de firma electrónica y de certificados partiendo de la norma técnica establecida a tal efecto en disposición adicional primera, que podrá convivir junto con otras políticas particulares para una transacción determinada en un contexto concreto" (el subrayado es nuestro).

3.2.3 La política marco de firma electrónica y de certificados; las políticas particulares

Finalmente, resulta preciso analizar el concepto de política marco (de firma electrónica), que no se establece como tal en el RDENI ni en su Norma Técnica de desarrollo, pero que se deriva de ambos.

La Guía de aplicación de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados es la encargada de explicitar la definición de política marco (Cfr. sección 8 de la Guía, 2011: p. 47.), como la "política de firma electrónica que puede servir como marco general de interoperabilidad para el desarrollo de políticas particulares con el objeto de cubrir necesidades específicas de las organizaciones para una transacción determinada en un contexto concreto, o bien para su adopción como política de firma electrónica por una organización", añadiendo que "las políticas marco pueden convivir junto con otras políticas particulares".

La noción de política marco se desprende, como hemos anticipado, del RDENI y, en concreto, de lo establecido en el artículo 18.1, cuando indica que "la Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad[174] para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación".

Cabe imaginar que la política marco de firma electrónica y de certificados a la que se refiere el artículo 18.1 del RDENI sea la misma que ya había previsto el artículo 24 del RDLAE, norma anterior en el tiempo a la aprobación del Esquema Nacional de Interoperabilidad.

Esta política ha sido ya aprobada por la Comisión Permanente del Consejo Superior de Administración Electrónica el 25 de octubre de 2010, en su versión 1.8[175]. Si bien no

[174] El subrayado es nuestro.

[175] Nótese que la versión inicial de la política de firma electrónica fue preparada el 21 de agosto de 2008, con bastante anterioridad a la aprobación del RDLAE y, por supuesto, el RDENI.

nos consta que se haya publicado en el Boletín Oficial del Estado, como exige el artículo 24.3 RDLAE, su texto se encuentra disponible[176], para consulta, en el Portal de la Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas.

Esta concreta política de firma electrónica, de acuerdo con lo establecido en el apartado 5 del artículo 18 del RDENI, "establecerá las características técnicas y operativas de la lista de prestadores de servicios de certificación de confianza que recogerá los certificados reconocidos e interoperables entre las Administraciones públicas y que se consideren fiables para cada nivel de aseguramiento concreto, tanto en el ámbito nacional como europeo", pudiendo "ser utilizada como referencia por otras Administraciones públicas para definir sus listas de servicios de confianza para aplicación dentro de sus ámbitos competenciales", previsiones que no han sido desarrolladas.

En las restantes Administraciones Públicas, existirá la posibilidad de definir (al menos) una, o varias, políticas marco de firma electrónica y de certificados, y alternativa o complementariamente, las políticas particulares que se consideren necesarias. Asimismo, en la Administración General del Estado también existirá la posibilidad de dictar políticas particulares de firma electrónica[177].

La existencia de una o varias políticas de firma electrónica no parece *a limine* generar problemas, en la medida en que todas ellas son reducibles a las reglas de la Norma Técnica de Interoperabilidad, pero la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración establece tres reglas referidas a las relaciones entre políticas, bajo el epígrafe II.5, denominado "interacción con otras políticas".

La primera regla del epígrafe II.5 establece que "cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de

[176] Se puede descargar la política de http://administracionelectronica.gob.es/es/ctt/politicafirma (última visita: 01/07/2012).

[177] Así se indica en la sección 2, p. 7, de la citada política, que indica que "esta política marco es global para toda la Administración Pública, y puede convivir junto con otras políticas particulares para una transacción determinada en un contexto concreto, siempre basadas en la política marco o global".

utilizar una política marco existente", regla orientada a evitar costes innecesarios y una posible inflación de documentos de política de firma electrónica. En efecto, parece absurdo crear una política de firma electrónica cuando se puede acudir a una política ya existente que sea perfectamente útil[178].

La segunda regla del epígrafe II.5 indica que "la definición del alcance y ámbito de aplicación de una política de firma electrónica se realizará considerando su interacción con otras políticas de firma electrónica, y asegurando que:

a) Su desarrollo es interoperable con la política marco, en caso de políticas de firma particulares.

b) Define las condiciones de utilización y convivencia con otras políticas particulares, si se trata de una política marco".

En el primer caso, la condición de desarrollo interoperable de la política particular con respecto a la política marco obliga a considerar a la política particular como una subpolítica de la política marco, cuando ésta exista[179]; esto es, la política marco debe cumplir la Norma Técnica de Interoperabilidad, mientras que la política particular debe cumplir la política marco, puesto que constituye una especificación de la misma a un caso concreto.

En el segundo caso, y de forma coherente, se impone a las organizaciones que dispongan de una política marco la determinación de las reglas aplicables a las políticas particulares, al objeto de evitar conflictos, en particular semánticos[180].

La tercera regla del epígrafe II.5, finalmente, establece reglas de tipo técnico

[178] Lo cual dependerá de cómo se preparen las políticas de firma electrónica, puesto que será más fácil adherirse a políticas genéricas, para casos de uso concretos, que a políticas con un fuerte contenido de tipo organizativo.

[179] De no existir una política marco, posibilidad que la regla a) del apartado 3 del epígrafe II.5 autoriza de forma implícita, entonces la política particular se debe configurar como una subpolítica de la propia Norma Técnica de Interoperabilidad.

[180] Como sucedería en caso de existir más de una política, marco o particular, aplicables de forma simultánea a una misma firma electrónica, lo cual la convertiría en "improcesable computacionalmente" y, por tanto, de imposible automatización.

orientadas a garantizar el correcto procesamiento de las políticas de firma electrónica marco y particulares, determinando que "en toda política de firma electrónica se asegurará que:

a) Las extensiones o restricciones establecidas para las reglas de creación o validación de firma atienden a la validación de los formatos de firma establecidos en esta NTI y política marco si procede, de forma que se garantice la interoperabilidad[181] entre las diferentes organizaciones.

b) Incluye[182], si procede, la referencia a la URL de la política marco de firma electrónica en la que se inscribe, con indicación expresa de la versión.

c) Las firmas que se generen siguiendo políticas marco o particulares, incluyen un campo donde se indique de forma explícita la política a la que pertenecen[183].

d) Para que otras aplicaciones puedan interpretar las reglas de una política particular correctamente, dicha política está disponible[184] en formato XML (eXtensible Markup Language) y ASN.1 (Abstract Syntax Notation One)".

[181] Como hemos visto anteriormente, la política de firma electrónica ha de ser una subpolítica de la política marco, y la política marco (o una política particular que no dependa de ninguna política marco) ha de ser una subpolítica de la Norma Técnica de Interoperabilidad.

[182] Nótese que esta inclusión se realizará en el documento electrónico que contiene la política de firma, mediante la técnica de la "incorporación por referencia". Así se explicita en la política marco de firma electrónica y de certificados de la Administración General del Estado, p. 7.

[183] Como veremos posteriormente, la forma típica de la firma electrónica que exige la Norma Técnica de Interoperabilidad es la denominada AdES-EPES, que efectivamente indica, aunque no sin problemas interpretativos, la política de firma electrónica aplicable a esa firma concreta. Resulta, en este sentido, remarcable que la política marco de firma electrónica de la AGE admita el empleo de la variante AdES-EPES implícita (Cfr. sección 2, p.8).

[184] Cfr. sección 3.4 de este trabajo, en relación con la publicación de las políticas de firma electrónica basadas en certificados.

3.3 LA NATURALEZA JURÍDICA DE LAS POLÍTICAS DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS

Analizado el concepto de política de firma electrónica y de certificados, debemos intentar establecer su naturaleza jurídica, a partir de los – escasos – datos normativos que la regulación nos ofrece.

El interés por una adecuada caracterización de la naturaleza de este instrumento es evidente, por cuando, como ha puesto de manifiesto MOLES PLAZA, 2004: pp. 36 y ss., los mecanismos de identificación y autenticación conforman una de las tipologías básicas de estructuras de control en Internet; en particular, por referirse al control de la identidad. En el caso de la criptografía y los certificados electrónicos, como hemos visto *supra*[185], la industria se ha autorregulado mediante la aprobación de un conjunto de especificaciones técnicas voluntarias en el ámbito del ETSI, bajo los auspicios de la Comisión Europea, que posteriormente se imponen a las Administraciones Públicas por la vía de la referencia a las mismas en una norma reglamentaria.

Recordemos que la política de firma electrónica y de certificados define el "conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma", según dispone la definición contenida en el anexo del RDENI.

Por tanto, parece que nos encontramos frente a un instrumento normativo, que regula el uso de la firma electrónica para un contexto dado, pudiendo ser de alcance general – como en el caso de una política marco prevista para una organización, o específico – como en el caso de una política particular.

La transmutación de las especificaciones técnicas voluntarias en norma reglamentaria y, por tanto, jurídicamente obligatoria supone, en nuestra opinión, una cierta

[185] Cfr. sección 3.1 de este trabajo, donde presentamos las especificaciones técnicas del ETSI en base a las cuales se ha definido la política de firma electrónica.

perversión del sistema de autorregulación, basado en el consenso, y deviene en un nuevo espacio de intervención autorregulada en origen sobre los cibernautas (MOLES PLAZA, 2004: p. 94). Espacio, sin embargo, en el que apreciamos con claridad el fenómeno descrito por ESTEVE PARDO, 2010: pp. 235 y ss., como deriva cientifista del Derecho, en particular por la remisión normativa a las soluciones de la ciencia y la tecnología.

En efecto, basta una lectura rápida de la "norma reglamentaria", o de las Decisiones de la Comisión Europea en materia de firma electrónica, para visualizar de inmediato la casi total dependencia que las mismas presentan de las especificaciones técnicas del ETSI, a las que constantemente se refieren: en materia de formatos técnicos para la longevidad de la firma electrónica, o de validez de los algoritmos o, finalmente, sobre sellado de fecha y hora.

En este sentido, el epígrafe I.1 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración indica que la misma "tiene por objeto establecer el conjunto de criterios comunes asumidos por la Administración pública en relación con la autenticación y el reconocimiento mutuo de firmas electrónicas basadas en certificados y que, como tales, serán desarrollados y consolidados a través de las políticas de firma electrónica basada en certificados", con el objetivo final[186] de "facilitar el uso de firmas electrónicas seguras e interoperables entre las distintas organizaciones de la Administración pública".

Además, en ambos casos, resulta que la política de firma electrónica y de certificados realmente establece, y de forma minuciosa y detallada, todas las condiciones aplicables a la firma electrónica de las transacciones realizadas por las Administraciones públicas.

Y lo hace con un carácter fuertemente prescriptivo, en atención a la cláusula de

[186] Este objetivo final sólo puede entenderse en el sentido de que la Norma Técnica persigue armonizar cómo crean las firmas electrónicas las Administraciones públicas, incluidas las relaciones que mantengan con los ciudadanos, para de esta forma poder intercambiar entre ellas los documentos producidos.

prevalencia del Esquema Nacional de Interoperabilidad contenida en el artículo 3.2 del RDENI[187], que no olvidemos es una norma básica de ineludible cumplimiento.

Estas reglas, en nuestra opinión, constituyen condiciones adicionales a la utilización de la firma electrónica en los procedimientos, reguladas en el artículo 4 de la LFE, debiendo cumplir los requerimientos aplicables[188] a las mismas, y en particular, "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".

De hecho, la previsión referida en el artículo 4.1 segundo párrafo de la LFE a "la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo" forma parte de la política de firma electrónica y de certificados, por prescripción de la Norma Técnica de Interoperabilidad que estamos estudiando.

Por su parte, otras reglas de la política de firma electrónica vienen moduladas por el derecho de admisión de los sistemas de firma electrónica basados en certificados[189], a tenor de las reglas de los artículos 21 de la LAE y 22 de la LUTICAJ, por lo que la Administración se mueve dentro de un ámbito de menor discrecionalidad. En concreto, el uso de los certificados reconocidos es un verdadero derecho de los firmantes[190], que no puede limitarse por vía de la política de firma electrónica, que en este caso sería ilegal[191].

---

[187] Dicho artículo dispone que "el Esquema Nacional de Interoperabilidad y sus normas de desarrollo, prevalecerán sobre cualquier otro criterio en materia de política de interoperabilidad en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos" (el subrayado es nuestro).

[188] Cfr. la sección 1.4 de este trabajo.

[189] Cfr. la sección 2.1 de este trabajo.

[190] Tanto de los ciudadanos cuanto de las Administraciones públicas.

[191] Y sin embargo, establece la regla primera del epígrafe IV.1 de la Norma Técnica de Interoperabilidad que "las políticas de firma, marco o particulares, podrán fijar limitaciones y restricciones específicas para los certificados electrónicos que admiten en cada uno de los servicios que corresponda, siempre en consideración de la normativa aplicable en cada caso", limitaciones y restricciones que deberán estar

Visto que la política de firma electrónica y de certificados de la Administración es, jurídicamente hablando, un conjunto de condiciones adicionales a la utilización de la firma electrónica en los procedimientos, resulta necesario dilucidar si se trata de condiciones adicionales generales o, por el contrario, de condiciones particulares. El interés práctico de la discusión es evidente, por cuanto – como sabemos – la aprobación de las condiciones adicionales generales exige una norma reglamentaria.

En este sentido, recordemos que el artículo 23.3 del RDLAE 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[192] y de Industria, Turismo y Comercio[193], previo informe del Consejo Superior de Administración Electrónica", mientras que el artículo 24.3 del RDLAE dispone que "la política de firma electrónica y certificados será aprobada por el Consejo Superior de Administración Electrónica". Y llama la atención que no se establezca previsión ninguna en el RDENI sobre el procedimiento o instrumento de aprobación de la política de firma electrónica y certificados.

Es decir, que para la aprobación de las condiciones generales adicionales se considera necesaria una norma reglamentaria, mientras que para la aprobación de la política de firma electrónica, que también son condiciones adicionales, se considera suficiente con un simple acto administrativo.

La posible dificultad se plantea precisamente en el caso de una política marco de firma electrónica y de certificados, dado que la misma se puede considerar equivalente a un conjunto de condiciones adicionales generales, y por tanto, exigir su aprobación por norma reglamentaria. Como hemos visto, por el contrario, la política marco de la Administración General del Estado se aprueba por un órgano colegiado como el

---

basadas en criterios verdaderamente estrictos para no incurrir en ilegalidad, especialmente desde el punto de vista del Derecho europeo.

[192] Esta competencia, en la actualidad, correspondería al Ministerio de Hacienda y Administraciones Públicas.

[193] Esta competencia, en la actualidad, correspondería al Ministerio de Industria, Energía y Turismo.

Consejo Superior de Administración Electrónica.

La explicación del diferente tratamiento jurídico que se produce en ambos casos se puede encontrar en el hecho de que la política de firma electrónica, sea marco o particular, realmente sólo concreta las condiciones aplicables a una firma electrónica, de entre las que han sido reglamentariamente establecidas por el RDENI y la Norma Técnica de Interoperabilidad que la desarrolla, por lo que no sería ya necesario acudir a una norma reglamentaria nueva.

En la misma línea, se puede entender que la política de firma no afecta realmente a los derechos de terceros, ya que se mueve dentro de los parámetros del derecho de admisión, legalmente regulado, por lo que únicamente concreta, mediante el correspondiente acto administrativo de decisión, las cuestiones técnicas aplicables a la firma electrónica que obviamente resultarán de necesario cumplimiento para el firmante y el verificador de la firma electrónica.

El último argumento en favor de la naturaleza no reglamentaria de las políticas de firma electrónica deriva de la propia naturaleza de la interoperabilidad, que se encuentra más cercana al establecimiento de acuerdos entre los participantes en procesos de intercambio que a la normalización por vía de imposición.

Esta lógica conduce a considerar la política de firma electrónica como una especie de convenio regulador de la operación de firma electrónica, que permite a las partes pactar las condiciones que aplicarán a la citada operación, y se deduce de la orientación colaborativa[194] del proceso de aprobación de la propia Norma Técnica de Interoperabilidad.

Sin embargo, la realidad es que en dicho "convenio" las partes no se encuentran en igualdad de condiciones: la Administración impone su política de firma electrónica a los ciudadanos o a las restantes Administraciones con quienes se relaciona[195], si bien lo

[194] Recordemos que la Norma Técnica de Interoperabilidad se elabora con la participación de todas las Administraciones Públicas a las que les es de aplicación, dentro del contexto del Comité Sectorial de Administración Electrónica.

[195] Nótese que el artículo 9.1 de la LAE, "cada Administración deberá facilitar el acceso de las restantes

hace dentro del marco de la Norma Técnica de Interoperabilidad.

3.4 LOS EFECTOS JURÍDICOS DE LA APLICACIÓN DE POLÍTICAS DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS

Cabe preguntarse, en último término, por los efectos jurídicos derivados de la aplicación de la política de firma electrónica y de certificados. Debemos, a estos efectos, diferenciar dos casos:

- Intercambio de documentos firmados, entre las Administraciones.
- Intercambio de documentos firmados, entre el ciudadano y la Administración.

3.4.1 Los efectos jurídicos en el intercambio de documentos entre las Administraciones

La norma de referencia es, este caso, el apartado 3 del artículo 18 del RDENI, el cual determina que "las Administraciones públicas receptoras de documentos electrónicos firmados permitirán la validación de las firmas electrónicas contra la política de firma indicada en la firma del documento electrónico, siempre que dicha política de firma se encuentre dentro de las admitidas por cada Administración pública para el reconocimiento mutuo o multilateral con otras Administraciones públicas".

Redactado desde la perspectiva de la organización que recibe una firma electrónica producida por otra organización, implica que dicha organización receptora debe aplicar las reglas de firma electrónica previstas en la política de firma electrónica que

---

Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad", por lo que su política de firma electrónica eventualmente se impone a la Administración que debe obtener acceso a los datos.

efectivamente se ha empleando en el momento de creación de la firma electrónica.

Esta necesidad nace de la existencia, que hemos visto anteriormente, de diversas políticas de firma electrónica. Normalmente será el firmante quien seleccione la política de firma electrónica que considere aplicable, y generará la firma cumpliendo los criterios técnicos exigibles en la misma.

Por su parte, el verificador de la firma deberá aplicar los mismos criterios técnicos a la verificación de la firma que el firmante, o de otra forma podría verificar incorrectamente la firma, lo cual generará errores e impedirá la correcta interoperabilidad del documento.

De ahí se deduce que firmante y verificados deben comunicarse y establecer la política aplicable, lo cual resulta poco conveniente, y genera un esfuerzo previo al inicio de los intercambios de documentos.

Para evitar esta barrera a la interoperabilidad, la Norma Técnica de Interoperabilidad apuesta porque la propia firma electrónica contenga la indicación a la política de firma aplicable al caso, motivo por el cual se impone la obligación de uso de la forma AdES-EPES, que incluye esta información[196].

Asimismo, el artículo 18.2 del RDENI y la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración obligan a la publicación de la correspondiente política de firma electrónica, como condición para su eficacia.

Aunque no se especifica en el RDENI, la regla 3ª.d) del epígrafe II.5 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración establece la política de firma electrónica se debe encontrar publicada

[196] La inclusión de la información de la política de firma electrónica aplicable se realiza en el momento de la creación de la firma electrónica, dado que resulta imprescindible que la firma electrónica del documento se extienda también a esta información, para evitar su sustitución o alteración anterior, y como prueba de que la citada política fue seleccionada o aceptada por el firmante. Cfr. regla II.5.3.c) de la Norma Técnica de Interoperabilidad de política de firma electrónica, ETSI TS 101733, sección 5.8.1 o ETSI TS 101903, sección 7.2.3.

en Internet, en lenguaje natural y también en XML y ASN.1, para su procesamiento automatizado por el verificador.

En este escenario, la organización que recibe el documento firmado sencillamente revisa la firma electrónica, obtiene el identificador de la política de firma electrónica, accede a la misma[197] y la aplica[198].

Un proceso aparentemente sencillo, pero que a fecha de hoy no se encuentra implantado de forma completa prácticamente en ninguna aplicación de las Administraciones Públicas, debido a su enorme complejidad técnica y semántica, lo cual exige aproximaciones parciales y pragmáticas a su implementación[199].

Son, en particular, las plataformas de validación las que están aplicando, en la actualidad, políticas de firma electrónica de forma normalizada en XML o ASN.1, incluyendo al menos la plataforma @firma[200] del Ministerio de Hacienda y Administraciones Públicas, y la plataforma PSIS de la Agència Catalana de Certificació / Consorci Administració Oberta de Catalunya.

Cabe preguntarse, también, por el tratamiento de una firma electrónica que no incorpore el campo indicativo de la política de firma electrónica (modalidad que se denomina AdES-BES). Nótese que, en consecuencia con la regla del artículo 18.3 del

---

[197] Lo cual no está exento de problemas – irónicamente – de interoperabilidad habida cuenta de la incompleta semántica de tratamiento de esta cuestión en ETSI TS 101733 y ETSI TS 101 903.

[198] La aplicación debería ser automática, a partir de la representación de la política de firma electrónica y de certificados en XML o ASN.1, si bien en la mayoría de casos actualmente implementados realmente lo que se hace es programar el sistema del verificador atendiendo a las reglas de la política de firma, en su versión en lenguaje natural (por ejemplo, así sucede en las facturas electrónicas). CROBIES, 2010: pp. 24 y ss. ofrece un modelo detallado para la representación de una política de firma electrónica en lenguaje natural.

[199] Así ha sido puesto de manifiesto en proyectos europeos de implantación de pilotos a gran escala, como PEPPOL, que en el ámbito de la contratación pública electrónica ha generado políticas de firma electrónica parcialmente procesables. Cfr. PEPPOL D1.3, 2012: pp. 14 y ss.

[200] Se puede acceder a las versiones en XML y ASN.1 de las políticas de firma electrónica de la Administración General del Estado en el Portal de Administración Electrónica, en http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=239 (última visita: 31/07/2012). Por cierto que dichas especificaciones no siguen fielmente (y en algún caso incumplen) las especificaciones técnicas del ETSI, lo cual no va a favorecer la interoperabilidad, incluso aceptando la necesidad de modificar dichas especificaciones técnicas por haber quedado manifiestamente desfasadas, que es nuestra posición en este asunto.

RDENI, dicha Administración no estaría obligada a aplicar ninguna política de firma electrónica en concreto, sino que podría aplicar su propia política marco de firma, o en su defecto, validar la firma aplicando las reglas generales de la Norma Técnica de Interoperabilidad.

Lo que no podría hacer, en nuestra opinión, es negarse a aceptar el documento firmado electrónicamente, en especial si el mismo procede de otro Estado de la Unión Europea, ya que las Decisiones dictadas en desarrollo de la Directiva de Servicios autorizan el empleo de AdES-BES o AdES-EPES indistintamente[201].

El mismo tratamiento debe recibir el documento que contiene una firma electrónica AdES-EPES implícita, ya que en este caso la política de firma electrónica aplicable viene determinada, con carácter general, por un contexto externo, como por ejemplo la semántica del documento al que se incorpora la firma o, más frecuentemente, la propia definición del formato documental empleado[202].

Finalmente, nos debemos interrogar por el tratamiento de una firma electrónica que contenga una política de firma electrónica que no cumpla las condiciones del artículo 18.3 *in fine*; es decir, que la misma no se encuentre dentro de las admitidas por cada Administración pública para el reconocimiento mutuo o multilateral con otras Administraciones públicas; o que incumpla el requisito de la publicación en Internet, por ejemplo.

En este caso, la Administración podría negarse a aceptar el documento firmado, alegando que no le resulta posible conocer o aplicar las condiciones marcadas por el firmante, efecto que parece jurídicamente razonable.

La cuestión a dilucidar, que la normativa no aclara, es qué debe entenderse por una política de firma electrónica admitida para el reconocimiento mutuo o multilateral, y

[201] En este caso, procedería aplicar directamente las reglas de la Decisión 2011/130/UE, en cuanto a formatos de firma electrónica, y de la Decisión 2009/767/CE, modificada por Decisión 2010/425/UE.

[202] Por ejemplo, la firma de documentos OOXML – ISO 29500, como Word 2010, se realiza empleando una firma XAdES-EPES implícita. Las reglas de la política de firma electrónica se deducen de lo descrito en dicha norma internacional.

de qué grado de discrecionalidad dispone la Administración en esta materia.

En nuestra opinión, y a pesar de la oscuridad de la norma, todas las políticas de firma electrónica que regulen sistemas de forma electrónica previstos en el artículo 21.1 de la LAE resultarían, en principio, admisibles para el reconocimiento mutuo o multilateral. Desde luego, asumiendo que ya existe un derecho de admisión al empleo de la firma electrónica, no resultaría en absoluto justificado limitarlo de forma discrecional.

Por el contrario, las políticas de firma electrónica que regulen sistemas de firma electrónica enmarcados en el artículo 21.2 de la LAE no deben disfrutar de esta admisión directa por otras Administraciones Públicas. En efecto, si una política de firma electrónica admite el uso de certificados reconocidos de pago, la misma no puede ser aplicada, como ya vimos al discutir el derecho de admisión, por una Administración diferente, que por tanto limitará la admisión de la política de firma electrónica igual que limita la admisión de la firma y del certificado.

En resumen, el efecto jurídico principal de la política de firma electrónica y de los certificados es, a tenor de lo que hemos visto, la aceptación obligatoria de la firma electrónica, tras la comprobación de su validez y aplicabilidad al caso concreto, o, por el contrario, la denegación motivada de la firma electrónica.

Se trata, como hemos visto *supra*[203], de un acto administrativo de producción automatizada, que en general se realizará en los sistemas cerrados de intercambio de documentos e informaciones que se establezcan entre las Administraciones actuantes.

El efecto jurídico secundario de la política de firma es la aceptación o denegación en el intercambio interadministrativo del documento electrónico que incorpora la firma, que en caso de denegación entendemos generará el correspondiente trámite administrativo de subsanación.

[203] Cfr. sección 2.3 de este trabajo.

3.4.2 Los efectos jurídicos en la relación electrónica del ciudadano con la Administración

Cabe ahora preguntarse por el efecto jurídico de la política de firma electrónica cuando se aplica la misma a la relación electrónica de un ciudadano con la Administración; es decir, determinar qué sucede cuando el mismo no cumpla lo establecido en la política de firma electrónica.

En este caso no resulta aplicable, a nuestro juicio, el artículo 18.3 del RDENI anteriormente analizado, pero de ello no se deriva que la política de firma electrónica no produzca efectos frente al ciudadano.

Más bien al contrario, precisamente la política de firma electrónica y de certificados que resulte aplicable al acto del ciudadano se convierte, en aplicación de las reglas generales del registro de entrada, en un elemento absolutamente clave.

Como hemos visto al estudiar la verificación de la firma electrónica como acto administrativo del procedimiento[204], cuando dicha verificación se realiza en el registro de entrada, generalmente de funcionamiento completamente automatizado (Cfr. REGO BLANCO, 2010: p. 556), resulta que el incumplimiento de la mayoría de los requisitos establecidos por la política de firma electrónica ya impediría la generación de la firma, puesto que normalmente es la Administración la que dispone los medios técnicos para la firma y presentación de los modelos normalizados, y por tanto, no resultaría posible proceder a la presentación del formulario electrónico, con el consiguiente efecto desfavorable para el interesado.

Como sabemos, al modelo normalizado cabe adjuntar otros documentos, que podrán ser de dos tipos:

- Documentos digitalizados por el presentador, según dispone el artículo 35.2 de

[204] Íbidem.

la LAE, que deberán incorporar firma electrónica avanzada o superior[205].

- Documentos originales electrónicos, firmados por su autor, que puede ser la Administración[206] o un ciudadano.

En nuestra opinión, en ambos casos resulta aplicable lo establecido en el artículo 25.4 de la LAE – por cierto, uno de los dos artículos de la ley que se remiten expresamente al Esquema Nacional de Interoperabilidad, salvedad hecha del artículo 42 que lo define –, que establece que "podrán aportarse documentos que acompañen a la correspondiente solicitud, escrito o comunicación, siempre que cumplan los estándares de formato y requisitos de seguridad que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad[207]", previsión legal que se podría interpretar en el sentido de sujetar estos documentos a la política de firma electrónica y de certificados de la Administración a la que se dirijan los mismos.

De hecho, precisamente el considerando primero de la Decisión de la Comisión Europea 2011/130/UE, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE, relativa a los servicios en el mercado interior, indica que "puede darse aún el caso de que los prestadores de servicios tengan que presentar documentos originales, copias compulsadas o traducciones compulsadas cuando efectúen dichos procedimientos y trámites. En estos casos, es posible que los prestadores de servicios tengan que presentar documentos firmados electrónicamente por autoridades competentes", por lo que establece reglas en este sentido, que han sido – incorrectamente en nuestra opinión – trasladadas a la Norma Técnica de

[205] Curiosa norma, que no parece encajar demasiado bien con la supuesta (y aclamada) neutralidad tecnológica respecto a los sistemas de firma electrónica del ciudadano, por cuanto aquí el legislador decide restringir, por ley formal, el uso de sistemas de inferior calidad: ¿Desconfía del ciudadano que se "autocompulsa" los documentos, o desconfía de los sistemas de firma electrónica que no son, al menos, avanzados?

[206] En puridad, las Administraciones deberían no solicitar documentos que otras Administraciones dispongan en forma electrónica, pero se puede prever que durante bastante tiempo esta norma se va a incumplir.

[207] El subrayado es nuestro.

Interoperabilidad de política de firma electrónica y de certificados de la Administración.

En efecto, como se dice en el considerando 3 de la citada Decisión, “para que los prestadores de servicios puedan llevar a cabo sus procedimientos y trámites por vía electrónica a través de las fronteras, es necesario garantizar que los Estados miembros puedan dar soporte técnico al menos a cierto número de formatos de firma electrónica avanzada cuando reciban documentos firmados electrónicamente por autoridades competentes de otros Estados miembros. La definición de cierto número de formatos de firma electrónica avanzada a los que tendría que dar soporte técnico un Estado miembro receptor facilitaría la automatización y mejoraría la interoperabilidad transfronteriza de los procedimientos electrónicos”, algo que nadie pone en duda.

Pero claro, trasladar esto con carácter general a la regulación española es, cuanto menos, arriesgado, porque no es lo mismo establecer requisitos para el intercambio entre autoridades competentes; esto es, en general Administraciones Públicas, que extender estos requisitos a los ciudadanos, que es lo que hace nuestra Norma Técnica de Interoperabilidad en su epígrafe III.3, regla 2ª, con importantes consecuencias prácticas en cuanto a los formatos documentales admitidos.

4 LAS NORMAS DE PROCESAMIENTO DE LA FIRMA ELECTRÓNICA

4.1 LOS INTERVINIENTES EN LOS PROCESOS DE FIRMA ELECTRÓNICA

El epígrafe II.3 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración se dedica a la identificación de los intervinientes en los procesos de firma electrónica, que son los siguientes:

- Firmante, al que define como la "persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa", siguiendo lo establecido en el artículo 6.2 de la LFE.

- Verificador, al que define como la "entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política de firma concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando", indicando también que podrá ser una entidad de validación de confianza[208] o una tercera parte que esté interesada en la validez de una firma electrónica.

  La LFE no contiene una definición de este actor, por lo que la Norma Técnica establece una definición propia, que en nuestra opinión cabe considerar defectuosa porque un verificador no tiene porqué emplear necesariamente una política de firma electrónica para la verificación de la firma electrónica, como hemos tenido ocasión de comprobar anteriormente[209].

  Además, esta definición introduce un aspecto referido a la semántica de la

[208] Esta entidad deberá cumplir los requisitos y condiciones que hemos estudiado en la sección 2.3.3 de este trabajo.

[209] Cfr. la sección 3.4.1 de este trabajo.

política de firma electrónica, cuando indica que la misma “rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando”, cuando realmente las determinaciones de la política de firma electrónica responden más bien al tipo de trámite que se realiza.

- Prestador de servicios de certificación, al que define como la “persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica”, también en línea con lo establecido en el artículo 2.2 de la LFE.

- Emisor y gestor de la política de firma, al que define como la “entidad que se encarga de generar y gestionar el documento de política de firma, por el cual se deben regir el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica”.

En relación con la gestión de la política de firma, el epígrafe II.6 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración define mediante tres reglas el conjunto de funciones y responsabilidades del gestor de la política.

En primer lugar, de acuerdo con la regla 1ª del epígrafe II.6, “la política de firma electrónica incluirá la descripción básica de su proceso de gestión, estableciendo las directrices para su mantenimiento, actualización y publicación, e identificando al responsable de llevar a cabo estas tareas”, previsión que se amplía en la regla 2ª del mismo epígrafe indicado los casos en los que se debe mantener actualizada la política de firma, que será la menos cuando se produzcan:

“a) Modificaciones motivadas por necesidades propias de la organización.

b) Cambios en políticas relacionadas.

c) Cambios en los certificados electrónicos emitidos por los prestadores de servicios de

certificación referenciados en la política de firma[210]".

Finalmente, la regla 3ª del epígrafe II.6 autoriza que "para facilitar la validación de firmas electrónicas creadas atendiendo a versiones anteriores de una política, se podrá mantener un repositorio con el historial de versiones anteriores que provea la ubicación de cada versión", previsión perfectamente aceptable que, sin embargo, plantea dificultades interpretativas ya en las propias especificaciones técnicas de referencia, por lo que puede ser de difícil cumplimiento práctico.

La determinación de los intervinientes es relativamente importante, ya que en relación a los mismos se establecen las reglas de la política de firma electrónica. En particular, sobre el firmante y el verificador se establecen las denominadas "reglas comunes" de firma electrónica, que el epígrafe III.1 de la Norma Técnica de Interoperabilidad de política de firma electrónica y certificados de la Administración caracteriza así: "Las reglas comunes permitirán establecer responsabilidades respecto a la firma electrónica sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados si son requisitos para el firmante, o no firmados si son requisitos para el verificador".

Las reglas comunes realmente definen las obligaciones informacionales de aportación de información a la firma electrónica por parte de firmante y verificador, por lo que su establecimiento presenta una dependencia evidente del formato de firma electrónica empleado en cada caso.

Esto es absolutamente lógico, porque es el modelo de procesamiento de la firma electrónica el que exige la actuación, en mayor o menor grado, de cada una de las partes intervinientes, pero también constituye una muestra de la función reguladora del código, según la construcción de LESSIG, 2006: pp. 226-232, que además en este

[210] Este punto es muy tributario de las especificaciones técnicas europeas de política de firma electrónica, en las que se obliga (sintácticamente) a incluir los puntos de confianza correspondientes a los certificados de los prestadores admitidos (cfr. ETSI TR 102 038 y ETSI TR 102 272). Sin embargo, con la aparición de las listas de confianza (TSL) resulta más simple sustituir estas referencias por la lista correspondiente, al menos en algunos escenarios. En este sentido, las versiones procesables informáticamente de la política de firma electrónica de la AGE, ya incluyen la TSL expedida por el supervisor estatal en lugar de todos los certificados admitidos.

caso ha llegado a informar la propia regulación jurídica, que se limita a describir el funcionamiento del programa, rendición del derecho ante la técnica que se plasma en la regla 2ª del epígrafe III.1 analizado, cuando indica que "estas reglas se definirán en base a los formatos de firma electrónica admitidos, teniendo en cuenta los diferentes usos de la firma electrónica basada en certificados, al uso de algoritmos y a los procesos de creación y validación de firma", todo ello definido por la industria sin la participación de los Estados.

4.2 LAS REGLAS SOBRE FORMATOS DE FIRMA ELECTRÓNICA

4.2.1 Las reglas generales de formatos de firma

Como hemos anticipado en el capítulo anterior, la Norma Técnica de Interoperabilidad es prolija en cuanto a los formatos de firma electrónica, quizá el aspecto de esta regulación que nos parece más criticable.

El epígrafe III.2 de la Norma Técnica se dedica al establecimiento de reglas en relación con los "formatos admitidos de firma electrónica", especificando diversas reglas de carácter general, que analizaremos seguidamente.

La regla 1ª de este epígrafe III.2 indica que "los formatos admitidos por las organizaciones para las firmas electrónicas basadas en certificados electrónicos, se ajustarán a las especificaciones de los estándares europeos relativos a los formatos de firma electrónica así como a lo establecido en la NTI de Catálogo de estándares".

Se trata de un texto verdaderamente oscuro. En primer lugar, porque hoy no existen propiamente "estándares europeos relativos a los formatos de firma electrónica", aunque cabe entender que se refiere a las especificaciones técnicas publicadas por el Instituto Europeo de Normas de Telecomunicaciones conocidas como XAdES, CAdES y PAdES.

Como es sabido, los estándares europeos producidos por el ETSI se identifican como

"ETSI ES" y el número de referencia, mientras que la especificaciones técnicas lo hacen como "ETSI TS" y el número de referencia, y el valor jurídico de unos y otras es diferente, por lo que quizá se debería haber sido un poco más estricto a la hora de establecer la regla del epígrafe III.2.1ª, que resulta de imposible cumplimiento, al menos en estos momentos.

Y en segundo lugar, porque remite, en igualdad de condiciones que a los estándares europeos, a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares, que no ha sido aún aprobada.

De la revisión del borrador[211] de la citada Norma se desprende la admisión de uso de los siguientes "estándares" de firma electrónica: CAdES, CMS, PAdES, PDF Signature[212], PKCS#7, XAdES y XML-DSig, como se puede ver con una cierta redundancia, pero un alcance más amplio, si bien el Catálogo de estándares no especifica para qué propósitos ni con qué restricciones se puede emplear cada uno de dichas especificaciones técnicas.

La regla 2ª del epígrafe III.2, por su parte, dispone que "los formatos de firma electrónica serán:

a) Estándares abiertos basados en estándares de firma europeos y ampliamente utilizados.

b) Seleccionados de entre los definidos por la Comisión Europea para la política de interoperabilidad de firmas electrónicas que será regulada a través de Decisión Comunitaria.

c) Compatibles con la definición de políticas de generación y validación de firmas para facilitar la interoperabilidad deseada y el automatismo en el tratamiento de firmas

[211] El texto del proyecto de resolución de Norma Técnica de Interoperabilidad se puede consultar en http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P60215901274203521811&langPae=es (última visita: 31/07/2012).

[212] Al cual, curiosamente, califica como de "uso generalizado". Curioso, teniendo en cuenta que una firma PDF es una firma CMS dentro de un fichero PDF (ISO 32000), ambos definidos por el propio texto como abiertos.

electrónicas generadas por distintas organizaciones.

d) Tales que permitan desarrollar funcionalidades avanzadas como la generación de firmas longevas de cara a garantizar su preservación.

e) Si procede, interoperables con la política marco en la que se basan".

Se trata de una norma, si cabe, aún más defectuosa que la anterior, y en nuestra opinión completamente desviada de todo propósito racional.

El apartado a) resulta redundante con la regla 1ª del mismo epígrafe III.2, si bien añade al hecho de emplear "estándares" abiertos el que sean "ampliamente utilizados", que es como no decir nada, especialmente en ausencia de estadísticas públicas sobre el uso de las especificaciones técnicas del ETSI en la Unión Europea.

El apartado b) sólo puede cualificarse como inseguro jurídicamente, en tanto en cuanto la selección de los citados estándares deberá hacerse conforme a un instrumento comunitario pendiente de aprobación. Parece que la referencia se estaría realizando a la Decisión 2011/130/UE, pero como la misma se cita en la propia Norma Técnica de Interoperabilidad, debemos entender que esta regla debe referirse a otra Decisión[213].

Respecto a los apartados c) y d), resulta evidente que están redactados, igual que los anteriores, para conducir al lector siempre hacia la adopción de los mismos estándares, que son precisamente los apuntados en la regla 1ª de este epígrafe III.3: XAdES, CAdES y PAdES, diseñados precisamente para estas finalidades[214].

En nuestra opinión, si se quería imponer el uso de XAdES, CAdES y PAdES, como veremos que se acaba haciendo en algunos casos, quizá hubiese sido más apropiado ordenarlo, dada la consideración del RDENI y las Normas Técnicas como normas

[213] Excepto si es, como por otra parte parece, un gazapo, en cuyo caso se agradecería la oportuna corrección de errores, en mor de intentar el cumplimiento de lo allí establecido.

[214] De hecho, y como hemos podido ver en la sección 3.1 de este trabajo, estas especificaciones técnicas son las que han creado y desarrollado los conceptos de política de firma electrónica o longevidad de firma electrónica, por lo que difícilmente se podrán seleccionar "estándares diferentes".

básicas en la materia.

Porque claro, la regla 3ª del epígrafe III.2 continua diciendo que "cada organización determinará los formatos y estructuras concretas de firma a incluir en su política, aplicando los criterios expuestos en esta NTI de forma proporcional al uso y necesidades de la firma electrónica en cada caso"; declaración que está muy bien, obviamente, por aquello de no parecer demasiado intrusivo, pero que en realidad no parece cierta, atendido el escaso margen de elección que todo este sistema deja a ciudadanos y Administraciones.

En el caso de la política de firma electrónica y de certificados de la Administración General del Estado[215], de forma previsible, los formatos escogidos para la firma electrónica son… XAdES y CAdES.

Pero no PAdES, si bien se indica que "se tendrá en consideración especial el formato PAdES (PDF Advanced Electronic Signatures), según especificación técnica ETSI TS 102 778-3, para su estudio y posible incorporación en futuras versiones de la política de firma, dada su especial relevancia como un formato de firma visible directamente por el ciudadano mediante herramientas estándar".

Pocos comentarios merecen las reglas 4ª y 5ª del epígrafe III.2, igual que el apartado e) de la regla 2ª[216] del mismo epígrafe, normas puramente organizativas llamadas, en especial la segunda, a cumplir la importante función de mantener alineados los sistemas técnicos con las nuevas versiones de las especificaciones técnicas de firma, que evolucionan de forma muy rápida[217].

[215] Cfr. la sección 2.2: pp. 8-9.

[216] Que dispone: "e) Si procede, interoperables con la política marco en la que se basan", en el sentido de que una política particular sólo podría elegir a partir de los formatos indicados en la política marco. Cfr. sección 3.2.3 de este trabajo.

[217] Como muestra, un botón: las especificaciones CAdES y XAdES referidas en la Norma Técnica de Interoperabilidad ha tenido que ser actualizadas en el ETSI debido al descubrimiento de problemas de procesamiento de algunos atributos de la forma -A, de forma que la Norma Técnica española ya ha quedado obsoleta.

4.2.2 Las reglas especiales de formatos de firma para transmisiones de datos

El epígrafe III.3 de la Norma Técnica de Interoperabilidad, en un ejercicio de realismo, se ha limitado a establecer, en su regla 1ª, que "la firma electrónica de transmisiones de datos estará basada en estándares recogidos en la NTI de Catálogo de estándares, siendo responsabilidad del emisor y gestor de la política la definición de las consideraciones concretas a aplicar por cada organización".

Cabe aquí referirse, como hemos visto en el análisis de la regla 1ª del epígrafe III.2, a estándares como PKCS#7 o CMS, que realmente son el mismo estándar pero en estadios diferentes de evolución, que se emplean en protocolos de transmisión de mensajes, como en el caso del correo electrónico seguro (S/MIME), o XML-DSig, muy utilizado en el aseguramiento de servicios web.

Y decimos que es un ejercicio de realismo, porque poco impacto tendría aquí el establecimiento de reglas por la Administración, dado el elevadísimo grado de autorregulación internacional del asunto, más allá de elegir entre las opciones que ofrece cada estándar, lo cual ni requiere de regulación alguna.

En consecuencia, la regla 2ª del epígrafe III.3 sencillamente considera una norma de tipo informativo, indicando que "cada política definirá las versiones soportadas así como los cambios en aquellas que pueden provocar una actualización de dicha política", que ningún comentario adicional requiere.

4.2.3 Las reglas especiales de formatos de firma de contenidos: ¿un injustificado obstáculo al empleo de estándares abiertos ofimáticos?

Por su parte, el epígrafe III.4 contiene el conjunto de reglas aplicable al tratamiento de la firma de contenidos.

Si bien la regla 1ª del epígrafe III.4 contiene un inocuo "en la política de firma se especificarán los formatos admitidos para la firma electrónica de contenido", la regla 2ª del mismo impone que "los formatos para la firma electrónica de contenido, atendiendo a la NTI de Catálogo de estándares, serán:

> a) XAdES (XML Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2.
>
> b) CAdES (CMS Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.4.
>
> c) PAdES (PDF Advanced Electronic Signatures), según la especificación técnica ETSI TS 102 778-3".

Se trata de una norma aparentemente correcta y razonable, por cuanto nadie duda de la adecuación de estas especificaciones técnicas del ETSI para representar, capturar y gestionar las informaciones que se consideran necesarias para el mantenimiento del valor legal de la firma electrónica a lo largo del tiempo.

El problema, sin embargo, viene dado por dos reglas concretas:

- En primer lugar, la regla 3ª del epígrafe III.4 determina que "el perfil mínimo de formato que se utilizará para la generación de firmas de contenido en el marco de una política será «-EPES», esto es, clase básica (BES) añadiendo información sobre la política de firma. En cualquier caso, cada organización podrá definir en su política de firma las consideraciones adicionales que considere respecto a la interpretación y utilización de diferentes perfiles y clases de los formatos

siempre en consonancia con lo establecido en esta NTI".

Ya nos hemos referido anteriormente[218] a los problemas de empleo de la firma electrónica con política, pero conviene hacer notar que se trata de un verdadero requerimiento, no de una simple recomendación.

- En segundo lugar, la regla 4ª del epígrafe III.4 determina que "las organizaciones aplicarán consideraciones de casos particulares para firma de contenido, al menos, en los siguientes casos:

  a) Los documentos electrónicos a los que se aplique firma basada en certificados de cara a su intercambio se ajustarán a las especificaciones de formato y estructura establecidas en la NTI de Documento electrónico.

  El formato de firma basada en certificados que acompaña a un documento electrónico se reflejará en el metadato mínimo obligatorio definido en la NTI de Documento electrónico 'Tipo de firma', que, en este caso, podrá tomar uno de los siguientes valores:

    i. XAdES internally detached signature.

    ii. XAdES enveloped signature.

    iii. CAdES detached/explicit signature.

    iv. CAdES attached/implicit signature.

    v. PAdES.

  b) La firma de facturas electrónicas según el formato «Facturae» se realizará conforme a lo regulado por la Orden PRE/2971/2007, de 5 de octubre."

Y, en concreto, deriva de la doble obligación de emplear estos, y no otros, subformatos de firma electrónica, según resulta de la Norma Técnica de Interoperabilidad de

[218] Cfr. sección 3.4.1 de este trabajo.

Documento electrónico, y del empleo de firmas con política explícita.

Porque si entendemos que estas normas aplican a los documentos a intercambiar entre los ciudadanos y las Administraciones, entonces la única conclusión posible es la imposibilidad de emplear ninguno de los estándares abiertos ofimáticos actualmente empleados, entre ellos ODF, base de aplicaciones como OpenOffice o LibreOffice, y OOXML, base de Microsoft Word 2010 y otras aplicaciones, en ambos casos estándares abiertos recogidos en el borrador de Norma Técnica de Interoperabilidad de Catálogo de estándares.

Hay que decir que los dos estándares a los que nos referimos implementan firmas electrónicas XAdES: ¿cuál es, entonces, el impedimento? Pues simple y llanamente, que dichas firmas XAdES implementan política implícita y que no son ni *internally detached*, ni *enveloped*, incumpliendo ambas reglas.

Respecto a la primera cuestión, hay que aclarar que, aunque estas firmas electrónica XAdES contienen el elemento *SignaturePolicy* exigido por la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración, no explicitan ninguna política de firma electrónica, ya que se acogen a una opción prevista en las especificaciones técnicas europeas de referencia, que permite indicar que la política de firma electrónica es "implícita" al documento.

Normalmente esto se produce porque es el propio estándar (abierto, en los dos casos citados) el que define la política de firma electrónica aplicable, que es local y concreta a la semántica de procesamiento del tipo documental estandarizado.

No se puede encontrar ninguna justificación a la discriminación de estos tipos de documentos firmados, especialmente cuando los mismos se presentan como anejos a una solicitud[219].

En lo que respecta a la segunda cuestión, es necesario indicar que el concepto de una

[219] Una solución al problema, en nuestra opinión, pasaría por aplicar la política de firma electrónica a la solicitud y aceptar los documentos anejos con su propia firma.

firma "XAdES *internally detached*" no existe como tal en las especificaciones técnicas europeas ni internacionales[220], por lo que no parece razonable esperar que el mercado produzca aplicaciones (o, más correctamente, formatos documentales complejos) que lo implementen, lo cual conduce al desarrollo de aplicaciones específicas por cada firmante o bien al empleo de aplicaciones ya desarrolladas, como el cliente @firma[221] o los componentes comunes de firma del Ministerio de Industria, Energía y Comercio[222].

No afecta sólo esta problemática a los dos estándares abiertos indicados, sino que potencialmente resulta aplicable a cualquier formato documental, por lo que en nuestra opinión, de ser ésta la interpretación que debe hacerse de la norma, sólo cabe indicar que la misma resulta manifiestamente ilegal, tanto en el ámbito doméstico[223] como, por supuesto, en el europeo[224].

[220] De hecho, una de las dos variantes de firma *internally detached* que soporta el cliente @firma, denominada "*internally detached* explícita" no está respaldada directamente por el estándar XMLDSig, como reconoce la documentación del producto (p. 12), lo cual generaría lógicos problemas de interoperabilidad.

[221] Disponible en el portal de administración electrónica del MINHAP, en la dirección http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=138 y que, por otra parte, ofrece funcionalidades de firma de documentos ODF y OOXML conforme a estándar, que obviamente no corresponden a la modalidad XAdES *internally detached*.

[222] Disponibles en http://oficinavirtual.mityc.es/componentes/ donde, por cierto, no se refieren a este subformato de firma electrónica como "*internally detached*" sino como "firma mixta", contribuyendo a una mayor confusión del público.

[223] Por infracción del derecho del ciudadano al uso de estándares abiertos, dada la total ausencia de justificación para el establecimiento de esta restricción.

[224] Por infracción de la Decisión 2011/130/UE, que no impone estos requisitos, por lo que resultan inoponibles a ciudadanos europeos que deban presentar documentos producidos por autoridades competentes de otros Estados.

4.3 LOS PROCESOS DE CREACIÓN Y VERIFICACIÓN DE LA FIRMA ELECTRÓNICA

4.3.1 Las reglas generales del Esquema Nacional de Interoperabilidad

Como hemos introducido ya[225], uno de los contenidos fundamentales de toda política de firma electrónica es, a tenor de la regla 2ª.a) del epígrafe II.1 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración, la definición de "los procesos de creación, validación y conservación de firmas electrónicas", definición que debe, por supuesto, realizarse dentro del marco de las reglas de la Norma Técnica.

En este sentido, la regla 3ª.c) del mismo epígrafe II.1 concreta que toda política de firma electrónica basada en certificados contendrá reglas comunes para el firmante y verificador, incluyendo reglas de creación de firma y reglas de verificación de firma, además de las reglas sobre formatos a las que nos acabamos de referir.

4.3.1.1 Las operaciones mínimas exigibles en la creación de la firma electrónica

Respecto a las reglas de creación de firma, en primer lugar indica la regla 1ª del epígrafe III.6 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración que "las políticas de firma definirán las condiciones particulares bajo las que, en su ámbito, se generará la firma electrónica", añadiendo a continuación la regla 2ª del mismo epígrafe las funcionalidades que deben ofrecer las plataformas que presten este servicio:

[225] Cfr. la sección 3.2.2 de este trabajo.

- Selección por parte del usuario firmante[226] del fichero, formulario u otro objeto binario para ser firmado, con indicación expresa de que los formatos de ficheros atenderán a lo recogido en la NTI de Catálogo de estándares (apartado a de la regla 2ª del epígrafe III.6).

  En este proceso, la plataforma debe permitir que el firmante se asegure de que el fichero que se quiere firmar no contiene contenido dinámico que afecte a su validez y que pudiese modificar el resultado de la firma a lo largo del tiempo, una norma que se orienta claramente a garantizar un máximo nivel de valor probatorio y eficacia del documento firmado[227].

- Realización de las siguientes verificaciones previas a la creación de la firma:

  - La firma electrónica puede ser validada para el formato del fichero específico que va a ser firmado, requisito que plantea problemas de interpretación dado que normalmente todos los ficheros se pueden firmar de diversas formas. Por ejemplo, un fichero ofimático se podría firmar con una firma específica de dicho formato, que se almacenaría dentro del propio formato documental, o mediante una firma independiente[228].

  - Los certificados a utilizar han sido expedidos bajo una Declaración de Políticas de Certificación específica y son certificados válidos según la legislación aplicable, requisito aparentemente sencillo que plantea bastantes retos de cumplimiento, tanto en relación con la declaración

[226] De esta redacción se desprende claramente la consideración del firmante como humano que se relaciona con el sistema mediante una interfaz, excluyéndose a los procesos automatizados, que quedan sin regulación directa, sin perjuicio de la posibilidad de aplicar, *mutatis mutandis*, estas mismas reglas.

[227] Así, por ejemplo, los documentos PDF 1.7 (ISO 32000-1) deben ser analizados de forma cuidadosa antes de su firma, ya que el estándar abierto ofrece múltiples opciones de contenido dinámico que, de no ser adecuadamente tratado y, en su caso, eliminado, podría afectar de forma efectiva al valor probatorio del documento electrónico firmado.

[228] Que se podría relacionar con el fichero firmado mediante una estructura contenedora en XML, registrando ambos elementos. En este caso, la firma electrónica sería *internally detached*.

aplicable[229] cuanto con la verificación de su validez[230].

- Validez del certificado, comprobando si el certificado ha sido revocado, o suspendido, si entra dentro de su periodo de validez, y la validación de la cadena de certificación, incluyendo la validación de todos los certificados en la cadena[231].

Resulta llamativa, a estos efectos, la previsión expresa de que "si no fuese posible realizar estas comprobaciones en el momento de la firma, será necesario, en todo caso, que los sistemas correspondientes asuman dicha validación, antes de aceptar el fichero, formulario u otro objeto binario firmado", que permite delegar al verificador parte de estas obligaciones y que en particular se debería aplicar para aliviar la carga de trabajo de la aplicación de firma que, por otra parte, en muchos casos es aportada por la Administración destinataria del documento firmado[232].

- Creación de un fichero con la firma según corresponda en función del formato utilizado, con la determinación adicional de que "en el momento de la firma, se incluirá la referencia del identificador único de la versión del documento de política de firma electrónica en el que se ha basado su creación", en una clara referencia adicional a la firma electrónica con política explícita a la que nos hemos referido con anterioridad.

---

[229] En este caso, el problema deriva de la no obligación de incluir esta información dentro del certificado, que sería la forma más fácil de comprobación automatizada. Cfr. la sección 6.4.1 de este trabajo.

[230] Dado que la validez del estado del certificado se trata en el siguiente punto, cabe entender que esta referencia debe entenderse hecha a que el certificado sea válido para este propósito particular; es decir, que sea un certificado reconocido, cuando dicha condición sea exigible, que contenga la información de identidad y, en su caso, de atributos, etc. Cfr. las secciones 2.1.2 y 6.3 de este trabajo.

[231] Carga que ya hemos estudiando anteriormente, en la sección 2.3 de este trabajo.

[232] Normalmente es en el registro electrónico, o alternativamente en el espacio de oficina virtual de trámites, donde se firma la solicitud empleando un *applet* de firma electrónica de la Administración, que por tanto implementa ya las previsiones de la política de firma electrónica correspondientes al trámite en cuestión.

4.3.1.2 Los contenidos mínimos y obligatorios de la firma electrónica

La regla 3ª del epígrafe III.6 de la Norma Técnica citada se ocupa, en línea con las previsiones anteriormente comentadas sobre formatos de firma electrónica, de indicar las informaciones que obligatoriamente debe registrar el firmante, y que se encuentran protegidas con su firma electrónica[233]:

- Fecha y hora de firma, que podrá ser meramente indicativa en función de cómo se haya generado la firma.

  Corresponde a la denominada "fecha alegada" de la firma, ya que se trata de una simple afirmación del momento de la firma electrónica, y no de un sello de fecha y hora sobre la firma. Puede ofrecer mayor o menos fiabilidad en función del entorno. Por ejemplo, si el equipo donde se genera la firma electrónica es de una organización que lo controla, y sincroniza la fecha y la hora de dicho equipo[234], la confianza que dicha organización tendrá en la fecha alegada de firma será muy superior que en el caso de una firma procedente de un equipo desconocido.

- Certificado del firmante, para evitar ataques de sustitución de dicho certificado que podrían comprometer el valor probatorio y la eficacia de la firma electrónica[235].

- Política de firma sobre la que se basa el proceso de generación de firma electrónica, requerimiento al que ya nos hemos referido anteriormente[236].

- Formato del objeto original, que contiene información que ayuda a la aplicación

[233] Motivo por el que únicamente el firmante puede aportarlos.

[234] Mediante el empleo de un cliente del protocolo NTP, por ejemplo, y una fuente de tiempo fiable corporativa, se puede ofrecer esta funcionalidad con elevadas garantías.

[235] Cfr. la sección 7.2.2 de la especificación ETSI TS 101903, por ejemplo.

[236] Cfr. la sección 3.4.1 de este trabajo.

a mostrar los datos a firmar a la persona firmante, al objeto de evitar errores en el procedimiento de creación de firma[237].

4.3.1.3 Los contenidos opcionales de la firma electrónica

Por su parte, la regla 4ª del epígrafe III.6 de la Norma Técnica citada se ocupa, también en línea con las previsiones anteriormente comentadas sobre formatos de firma electrónica, de indicar las informaciones que opcionalmente puede registrar el firmante, y que, en este caso, se encontrarán protegidas con su firma electrónica:

- Lugar geográfico donde se ha realizado la firma del documento, elemento de semántica compleja y efecto jurídico de difícil previsión, que debemos entender aplicable en el contexto de la determinación de la ley aplicable y de la jurisdicción competente, en especial en al ámbito del derecho internacional privado[238], si bien su utilidad en el caso del procedimiento administrativo electrónico puede resultar más escasa.

- Rol de la persona firmante en la firma electrónica, que permite la inclusión de un rol alegado o certificado. En el primer caso, se trata simplemente de una cadena de texto[239] que denota el rol, mientras que en el segundo, se trata de un certificado de atributos que garantiza el citado rol, posibilidad que no

[237] Se trata de un elemento que, aunque recomendado, no es obligatorio en las especificaciones técnicas europeas de referencia (cfr. por ejemplo, la sección 7.2.5 de ETSI TS 101 903), por lo que su inclusión puede generar algunos problemas de neutralidad tecnológica, aunque en menor grado e importancia que en otros aspectos de la Norma Técnica de Interoperabilidad analizada.

[238] En efecto, la indicación del lugar de producción de la firma podría ser un indicio que ayude a la determinación de la ley aplicable o de la jurisdicción competente, pero no es menos cierto que también puede ser un factor internacionalmente equivalente, e incluso de distorsión. Las reglas de derecho internacional privado suelen establecer la libertad de las partes respecto al establecimiento de la ley aplicable a un contrato, así como primar la aplicación de la ley del Estado de residencia habitual de los consumidores, por ejemplo, pero no suelen acudir a *la lex loci celebrationis* con facilidad, por lo que este elemento se debería estudiar con un cierto detalle antes de su empleo.

[239] Esta cadena puede estar preestablecida en la política de firma electrónica, como sucede en el caso de la política de factura electrónica publicada por la Administración General del Estado, o ser tecleada por el propio firmante, en cuyo caso se complica el procesamiento del rol, en especial el automatizado, que puede devenir imposible por problemas semánticos.

permite emplear la actual Norma Técnica de Interoperabilidad[240].

- Acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.), que permite establecer una semántica específica en relación con la política de firma electrónica y, por tanto, a las firmas electrónicas producidas, así como modular las reglas aplicables en cada caso, de forma que las firmas electrónicas sólo serán válidas si se cumplen las reglas de dicha "acción" del firmante[241].

- Sello de tiempo sobre algunos o todos los objetos de la firma, que permite, entre otras técnicas, mantener el valor probatorio de la firma electrónica, según veremos[242].

Otro contenido opcional de firma electrónica que debe aportar el firmante lo encontramos en la regla 6ª del epígrafe III.6 de la Norma Técnica, que indica, de forma algo críptica, que "en caso de creación de firmas electrónicas por distintos firmantes sobre un mismo objeto, donde el segundo firmante ratifica la firma del primero se utilizará la etiqueta correspondiente, CounterSignature, para contabilizarlas".

Lo que quiere decir el texto, a la luz de las correspondientes especificaciones técnicas europeas de referencia, es que de los diferentes métodos que existen para generar estas secuencias de firmas sobre firmas, se debe emplear uno en concreto, en el caso de la firmas en XML teóricamente por su mayor compatibilidad con XMLDSig, sin que en nuestra opinión sea una justificación suficiente para establecer esta restricción técnica.

---

[240] Sobre la problemática de los certificados de atributos en la firma electrónica, cfr. la sección 6.3.1 de este trabajo.

[241] En las especificaciones técnicas europeas de referencia este elemento se denomina "tipo de compromiso del firmante" y permite establecer una significación concreta para la firma electrónica, de forma que la aceptación de la firma verificada implica la aceptación de la semántica del compromiso indicado. Nótese que cada política de firma electrónica puede definir tipos de compromiso, con su propia semántica, o empelar tipos de compromiso registrados por organizaciones, en cuyo caso se deberá estar a la semántica establecida por la organización registradora. Un ejemplo de compromiso es "prueba de origen", "prueba de recepción", "prueba de envío"…. Cfr. la sección 7.2.6 de la especificación ETSI 101 903, por ejemplo.

[242] Cfr. la sección 4.4 de este trabajo.

También el verificador puede aportar contenidos opcionales a la firma electrónica, como determinan las especificaciones técnicas europeas de referencia, y de hecho, la denominada "firma electrónica longeva" se basa precisamente en el completado de la firma electrónica mediante la recolección y aportación de estas informaciones, por el verificador, a la estructura de la firma electrónica, según veremos[243].

4.3.1.4 Las operaciones mínimas exigibles en la validación de la firma electrónica

Respecto a las reglas de verificación de firma, en primer lugar indica la regla 1ª del epígrafe III.7 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración que "las políticas de firma definirán las condiciones particulares bajo las que, en su ámbito, será posible validar la firma electrónica de un documento", añadiendo a continuación la regla 3ª del mismo epígrafe III.7 las funcionalidades que deben ofrecer las plataformas que presten este servicio:

- Garantía de que la firma es válida para el fichero específico que está firmado, que debemos entender en cuanto a la comprobación matemática de la firma empleando la función de verificación del algoritmo de firma electrónica mediante la clave[244] correspondiente.

- Validez de los certificados, para lo cual resulta imprescindible disponer de un referente temporal conforme al que calcular si en ese momento el certificado era válido. Imaginemos, por ejemplo, una firma electrónica producida el 1 de septiembre de 2012 que se precisa verificar el 1 de septiembre de 2020, momento en el que el certificado reconocido en el que se basa ha perdido, en

[243] Cfr. la sección 4.4 de este trabajo.

[244] Recuérdese que la clave pública se emplear para comprobar la firma electrónica generada con la clave privada (cfr. la sección 5.2.1 de este trabajo), y que dicha clave pública se encuentra dentro del certificado (cfr. la sección 6.1.1 de este trabajo).

todo caso, su validez[245].

En este sentido, la Norma Técnica es bastante prolija:

- Se debe emplear, para la validación, la fecha de producción de la firma (1 de septiembre de 2012) si se da cualquiera de estas circunstancias:

  - Si los servicios de los prestadores facilitan los históricos de estado de los certificados y la firma lleva un sello de tiempo válido en el momento de la verificación.

    Como se puede ver, se requiere disponer de acceso a la información de estado de certificados, que ya se encontrará archivada[246], y también que la garantía de que la fecha de producción de la firma es verídica, mediante el sello de fecha y hora, que debe encontrarse vigente[247].

  - Si se trata de firmas longevas que incluyen las evidencias de la validez de la firma electrónica en el momento de la generación o primera validación, y dichas evidencias se encuentran selladas con un sello de tiempo válido.

    Como en el caso anterior, se precisa de la información de estado de certificados, que en este caso se encuentra incorporada

[245] Dado que un certificado reconocido no puede, por mandato legal, durar más de cuatro años, habrá expirado antes de la fecha de validación (cfr. artículo 8.2 de la LFE).

[246] El artículo 20.1.f) de la LFE obliga a los prestadores de servicios de certificación que expidan certificados reconocidos a "conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo", pero desde luego esta previsión no se ha interpretado por el mercado en el sentido de mantener publicadas las listas de revocación de certificados durante esos quince años, sino que más bien se retiran de dichas listas los certificados suspendidos o revocados cuando los mismos hubiesen expirado, por cuestiones de espacio y eficiencia computacional.

[247] La vigencia del sello de fecha y hora depende de la duración del certificado que emplea el prestador de servicios de certificación para su firma, por lo que debe revisarse cuidadosamente la duración del mismo en el momento de su incorporación a la firma, empleando el elemento SignatureTimeStamp (cfr. la sección 7.3 de ETSI TS 101 903, por ejemplo).

dentro de la firma que se valida[248], y garantía de autenticidad de dicha información, mediante un sello de tiempo también válido[249], debe entenderse que en el momento de la validación de la firma electrónica.

- En caso contrario, la firma se debe verificar contra la fecha de la verificación (2 de septiembre de 2020), por lo que en el ejemplo que estamos empleando para ilustrar este punto, la firma sería reputada inválida.

- Las comprobaciones a realizar incluyen "que los certificados no fueron revocados ni suspendidos y que no han expirado", entendiéndose que a la fecha anteriormente determinada, para lo cual se deberá consultar la información histórica de estado, o la información de validación que se obtuvo en su día y fue incluida en la firma electrónica longeva.

  A esta regla debe añadirse la prevista en la regla 5ª del epígrafe IV.1 de la misma Norma Técnica, en virtud de la cual "la política de firma electrónica podrá establecer el período de precaución o de gracia que corresponda aplicar para la validación de los certificados. Este periodo podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (Certificate Revocation Lists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol)", regla que indica que, en general, la comprobación de los certificados se podrá diferir en el tiempo, en función del mecanismo empleado, entre pocos minutos (OCSP) hasta 24 horas (CRL), ya que las prácticas actuales permiten dichos periodos para

[248] Esta incorporación se realiza mediante diversos elementos propios de la firma longeva (cfr. la sección 4.4 de este trabajo).

[249] Esta referencia debe entenderse realizada a diversos tipos de sello de fecha y hora sobre evidencias de validez de la firma electrónica, como veremos al tratar la firma longeva (cfr. la sección 4.4 de este trabajo).

el refresco de la información de estado[250].

Esto implica que algunas firmas electrónicas[251] presentadas en aplicaciones como el registro electrónico de entrada de documentos de la Administración pueden no ser verificadas de forma definitiva hasta el día siguiente a su presentación, por lo que se deberán recibir los documentos "salvo buen fin", realizando una validación parcial de la firma electrónica, y proceder a realizar una validación definitiva cuando la información de estado se encuentre disponible.

Si de la validación definitiva se desprende la invalidez del certificado y, por consiguiente, de la firma, se deberá solicitar la correspondiente subsanación, en los términos del artículo 71 de la LRJPAC, ya que en este caso no se puede tener la presentación por no realizada[252].

- Además, "se comprobará la validez de toda la cadena de certificación, incluyendo todos los certificados que la componen, con independencia de que éstos se encuentren incluidos en la propia firma o no", dado que en la firma sólo es obligatorio, como hemos visto, incluir el certificado del firmante, pero no necesariamente los certificados de autoridad de certificación. En caso de no haberse incluido en la firma electrónica, obviamente se deberá disponer de acceso a los citados certificados[253].

- Más dudas genera la obligación en virtud de la cual "se verificará que el certificado ha sido expedido por un prestador de servicios de certificación de confianza bajo una Declaración de Prácticas de

[250] Cfr. ETSI TS 101 456, especificación de referencia para la expedición y gestión de certificados electrónicos reconocidos, sección 7.3.6.a).

[251] Al menos, las que sólo se puedan verificar empleando CRL.

[252] En efecto, el presentador ha obtenido el correspondiente recibo del registro electrónico, por lo que considerar que no se ha producido la presentación le situaría en una clara situación de indefensión frente a la Administración.

[253] A medida que transcurre el tiempo, puede ser un riesgo incremental, especialmente en atención a la posibilidad de cese en la actividad por el prestador del servicio de certificación, a tenor de la regulación contenida en el artículo 21 de la LFE.

Certificación que cumplirá la normativa y estará incluido en la política de firma aplicable", como hemos indicado anteriormente, especialmente en el caso de la automatización de la citada comprobación, excepto si este control se aplica en el momento de "admisión" del prestador de servicios de certificación, y su correspondiente inclusión en la política de firma electrónica aplicable.

- Finalmente, se deberá proceder a la "verificación, si existen y si así lo requiere la política de la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos", norma que resulta ciertamente sorprendente. Si no se verifican los sellos de fecha y hora de los formatos de firma electrónica, no se puede confiar en que los mismos sean veraces o fiables, con lo cual tampoco se podrá confiar en las informaciones de firma y verificación de firma que los mismos salvaguardan.

Respecto a las contrafirmas, la regla 5ª del epígrafe III.7 de la Norma Técnica en cuestión únicamente indica que "si se han realizado varias firmas sobre un mismo documento, se seguirá el mismo proceso de verificación que con la primera firma, comprobando cada firma o la etiqueta CounterSignature en el campo de propiedades no firmadas, donde se informa de los refrendos de firma generados", de forma análoga al mecanismo ya comentado en la creación de la firma electrónica, por lo que no requiere de mayor análisis.

4.3.2 Las reglas adicionales del Esquema Nacional de Seguridad

No es sólo, como hemos indicado ya, el Esquema Nacional de Seguridad el instrumento regulador de los procesos de firma electrónica, sino que también el artículo 33 del RDENS indica, en su apartado primero, que "los mecanismos de firma electrónica se aplicarán en los términos indicados en el Anexo II de esta norma y de acuerdo con lo preceptuado en la política de firma electrónica y de certificados, según se establece en

el Esquema Nacional de Interoperabilidad", mientras que el segundo apartado del propio artículo detalla que "la política de firma electrónica y de certificados concretará los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas, sin perjuicio de lo previsto en el Anexo II, que deberá adaptarse a cada circunstancia".

La firma electrónica se trata, por tanto, en esta norma en su consideración de medida de seguridad, aplicable, en particular a la protección de los activos en sus dimensiones de autenticidad[254] e integridad[255], en una regulación que obviamente se solapa, ya que difícilmente se pueden imaginar actos del procedimiento administrativo que sólo se encuentren sujetas a uno de ambos reglamentos.

En este sentido, para establecer de forma completa el conjunto de reglas aplicables a los procesos de firma, se debe determinar la categoría de seguridad del sistema, de acuerdo con las reglas del artículo 43 y anexo I del RDENS, a partir del nivel de seguridad requerido en las diferentes dimensiones de seguridad: "Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para

[254] El RDENS la define, en su anexo IV, como la "propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos".

[255] El RDENS la define, en su anexo IV, como la "propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada".

atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.

2.º El sufrimiento de un daño menor por los activos de la organización.

3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.

4.º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.

5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

1.º La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.

2.º El sufrimiento de un daño significativo por los activos de la organización.

3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.

4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.

5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1.º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.

2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

3.º El incumplimiento grave de alguna ley o regulación.

4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

5.º Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio".

En general, podemos prever que, en la mayoría de procedimientos administrativos, el nivel de seguridad necesario en las dimensiones de autenticidad e integridad de los documentos administrativos será bajo, al menos aplicando el criterio general de que los defectos formales en la producción de documentos administrativos son, en general, irregularidades no invalidantes.

A pesar de esta primera caracterización, lo cierto es que otros argumentos conducen a exigir el nivel medio de seguridad en estas dimensiones: por ejemplo, en caso de admitir un sistema criptográfico utilizado para el acceso a informaciones administrativas por parte de los ciudadanos, o por otras Administraciones, si se diese un error en la identificación del suscriptor por el prestador se vulneraría la legislación de protección de datos personales, porque se habría divulgado información personal a persona no autorizada, lo cual es una infracción material de la ley. También en el caso de una solicitud de inicio de procedimiento donde se solicita que las notificaciones se realicen de forma electrónica nos encontraríamos, en caso de incidente, en una infracción de la norma, en este caso al menos por tratarse de una irregularidad formal

insubsanable, generadora de indefensión.

Habida cuenta que estas dos posibilidades se dan, con carácter general, en la práctica totalidad de los procedimientos administrativos iniciados de oficio, cabe apostar por la cualificación de los sistemas como de nivel medio, sin perjuicio de que, en función de los trámites, algunos puedan ser de nivel bajo o, más raramente, alto.

Las reglas concretas que establece el RDENS para cada nivel de seguridad se presentan a continuación:

- En el nivel bajo, se podrá emplear cualquier medio de firma electrónica de los previstos en la legislación vigente.
- En el nivel medio, los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada. En todo caso:
    - Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
    - Se emplearán, preferentemente, certificados reconocidos.
    - Se emplearán, preferentemente, dispositivos seguros de firma.
    - Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la política de firma electrónica y de certificados que sea de aplicación. Para tal fin:
        - a) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo los certificados y los datos de verificación y validación.
        - b) Se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.
        - c) El organismo que recabe documentos firmados por el

administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes a) y b).

- d) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes a) y b).

- En el nivel alto, se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en el nivel medio, además de las siguientes:
  - a) Se usarán certificados reconocidos.
  - b) Se usarán dispositivos seguros de creación de firma.
  - c) Se emplearán, preferentemente, productos certificados [op.pl.5]".

Como se puede ver, no hay grandes novedades con respecto a las reglas generales contenidas en la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración, pero hay que reconocer que aporta un criterio para decidir el grado apropiado de seguridad que se requiere en cada tipo de actuación administrativa, entendida en su consideración de servicio, y a cada tipo de documento del procedimiento, en su consideración de información, como activos que son de la Administración.

En este sentido, y a reserva de los comentarios concretos que realizaremos a algunas de las reglas anteriores, en sede de política criptográfica y de uso de certificados, resulta un complemento interesante para la Norma Técnica de Interoperabilidad analizada, y permite realizar el equilibrio entre los principios de seguridad y proporcionalidad que informan la legislación.

Así, a título de ejemplo, cabe reflexionar sobre la no necesidad de emplear certificados electrónicos reconocidos ni dispositivos seguros de creación de firma electrónica salvo en el nivel alto de seguridad, lo cual resulta apropiado en términos de seguridad, pero debe cohonestarse con el derecho del ciudadano a emplear dicho certificado, si lo

posee y entra dentro de los parámetros del derecho de admisión.

4.4 LA CONSERVACIÓN A LARGO PLAZO DE LA FIRMA ELECTRÓNICA

Uno de los problemas importantes de la firma electrónica deriva de la obsolescencia de las cifras criptográficas, que afecta a la validez matemática de las firma electrónicas generadas en el pasado y, por tanto, genera un problema evidente respecto a la perdurabilidad de los documentos firmados electrónicamente, especialmente en relación con el valor probatorio de los citados documentos.

La Norma Técnica de Interoperabilidad dedica diversos epígrafes a esta cuestión.

Para empezar, el epígrafe II.7, sobre archivado y custodia, indica en su regla 1ª que "atendiendo a las necesidades y normativa específicas de su ámbito, las políticas de firma podrán contemplar la definición de condiciones y responsabilidades para el archivado y custodia de las firmas electrónicas en sus diferentes aplicaciones", para posteriormente autorizar, en su regla 2ª, los siguientes métodos de conservación:

- Las denominadas "firmas longevas".
- Otros métodos, que podemos englobar en la denominación genérica de "repositorio seguro".

La elección de uno u otro mecanismo es responsabilidad de la entidad gestora de la política de firma electrónica, en nuestra opinión, siendo relevante indicar que, de acuerdo con la regla 6ª del epígrafe II.7 de la Norma Técnica, "la definición de medidas y procedimientos para archivado y custodia de firmas electrónicas se realizará atendiendo con proporcionalidad a los diferentes usos de la firma electrónica contemplados en el alcance y ámbito de aplicación de la política", lo cual exige un análisis de las necesidades de conservación de los documentos firmados electrónicamente, en los términos dispuestos por la normativa de gestión de documentos de archivo correspondiente, y la aplicación de "lo establecido en la NTI de Política de gestión de documentos electrónicos" (regla 7ª del epígrafe II.7).

Reiterativa resulta, por tanto, la regla 4ª del epígrafe IV.3 de la Norma Técnica cuando insiste en que "las políticas de firma contemplarán la definición de formatos y consideraciones de uso de firmas longevas conforme a las necesidades específicas de su ámbito de aplicación y a la normativa específica aplicable".

4.4.1 La conservación mediante firmas longevas

La Norma Técnica de Interoperabilidad de política de firma electrónica no define qué sea una firma electrónica longeva, si bien la describe en su regla 2ª.a) del epígrafe II.7, en el siguiente sentido: "firmas longevas mediante las que se añadirá información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza, aplicando las reglas de confianza para firmas longevas descritas en el subapartado IV.3", caracterización que resulta necesario completar con las restantes previsiones de la norma.

La regla 3ª del epígrafe II.7 indica que "cada política de firma definirá un servicio para mantener las evidencias de validez de las firmas longevas y gestionar la actualización de las firmas", de lo cual se desprende la caracterización de la firma electrónica longeva como una firma que ha sido completada. En este sentido, la misma regla 3ª indica que "dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma como los certificados e informaciones de estado utilizadas en su validación", apuntando los elementos que se contienen en la firma electrónica longeva.

La regla 4ª del mismo epígrafe II.7 ofrece algo más de información, cuando indica que "el almacenamiento de los certificados y las informaciones de estado podrá realizarse dentro del fichero resultante de la firma electrónica […]: a) En caso de almacenar los certificados y las informaciones de estado dentro de la firma, se sellarán también dichas informaciones, siguiendo las modalidades de firmas AdES -X o –A", de o cual se deduce que la firma longeva se corresponde con dichos formatos de firma, definidos en las correspondientes especificaciones técnicas europeas de referencia.

Sin embargo, es la regla 5ª del epígrafe II.7 la que aclara de forma más completa la

finalidad de la firma electrónica longeva, cuando establece que “la protección de la firma electrónica frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez, se realizará a través de uno de los siguientes procesos: a) Utilización de mecanismos de resellado, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de fecha y hora de archivo con un algoritmo más robusto”, pudiendo asimismo “las políticas de firma […] definir la aplicación de mecanismos de resellado para facilitar la conservación de la firma electrónica”.

En efecto, la longevidad de la firma electrónica se logra mediante la protección técnica de la firma electrónica empleados sellos de fecha y hora, siguiendo lo establecido en las especificaciones técnicas europeas de referencia.

En este sentido, la regla 1ª del epígrafe IV.3 de la Norma Técnica de Interoperabilidad de política de firma electrónica establece que “en el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma”, mediante el elemento SignatureTimeStamp, aspecto que se aclara en las especificaciones técnicas aplicables.

Si bien la Norma Técnica no explicita en las razones técnicas de esta aproximación, se pueden deducir con facilidad de las citadas especificaciones técnicas, así como de las reglas de validación de firma prevista en la Norma. En concreto, se recordará que el aspecto más relevante en la validación de la firma electrónica era la determinación del momento de producción de la firma, para poder comprobar su corrección empleando certificados que eran válidos en el momento de creación de la firma, pero que ya han perdido su validez por el transcurso del tiempo.

Nótese que como las referencias a las informaciones de estado de certificados también se encuentran firmadas, con carácter general, su validez también se puede perder a largo del tiempo y, por tanto, deben ser también protegidas por los sellos de fecha y hora.

Por este motivo, la regla 2ª del epígrafe IV.3 determina que “para la conversión de una

firma electrónica a firma electrónica longeva:

a) Se verificará la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES y las referencias.

b) Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:

> i. Certificados: incluyendo los certificados del firmante y de la cadena de certificación.
>
> ii. Informaciones de estado de los certificados, CRLs o las respuestas OCSP[256].

c) Aplicación del sellado a las referencias a los certificados y a las informaciones de estado", mediante diversos elementos disponibles a tal efecto, que convierten la firma al perfil AdES-X (firma electrónica extensa), –XL (firma electrónica súper extensa) o –A (firma electrónica de archivo, que se identifica con la firma electrónica longeva en este epígrafe).

El verdadero problema reside en que también los sellos de fecha y hora son documentos firmados electrónicamente y, por tanto, su validez también es limitada en el tiempo, lo cual exige la incorporación periódica de nuevos sellos de fecha y hora que protejan todas las informaciones anteriormente referidas. A este fenómeno se conoce como "resellado", y para soportarlo técnicamente se emplea el elemento ArchiveTimeStamp definido en las especificaciones técnicas europeas de referencia (existente únicamente en firmas AdES –A).

En principio sería suficiente con incorporar un sello de fecha y hora[257] de archivo de larga duración, para lo cual se precisa que su algoritmo sea ciertamente robusto, y

[256] La regla 3ª del mismo epígrafe IV.3 reitera esta cuestión, cuando indica que "para la incorporación a la firma de la información completa de validación, se usará validación mediante CRLs u OCSP".

[257] Nótese que la regla 4ª del epígrafe IV.2 de la Norma Técnica indica que "los sellos de tiempo seguirán las especificaciones técnicas establecidas en el estándar ETSI TS 102 023, «Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities»", al objeto que los mismos ofrezcan unas condiciones suficientes de seguridad y calidad.

emplear una clave de longitud elevada[258]. Mientras dicho algoritmo y clave se mantengan vigentes, no resultará necesario añadir un nuevo sello de fecha y hora.

4.4.2 La conservación mediante repositorio seguro

La Norma Técnica permite también la conservación de la firma electrónica, mediante "otros métodos técnicos que impedirán la modificación de la firma para la que se ha verificado su validez, de acuerdo a los requisitos establecidos en la política de firma correspondiente, y que habrá sido almacenada en un sistema en un momento del tiempo determinado", según autoriza la regla 2ª.b) del epígrafe II.7, de forma alineada con la previsión equivalente que se encuentra en las normas técnicas europeas de referencia, generalmente conocida como "secure records", pero que en nuestra opinión se identifica de forma más apropiada con el concepto de "repositorio seguro".

La misma regla continúa indicando que "todos los cambios que se realicen sobre el sistema en el que se encuentra almacenada la firma podrán auditarse para asegurar que dicha firma no ha sido modificada", norma complementaria de la anterior.

Asimismo, se establece que "los requisitos de seguridad de dichos sistemas cumplirán con las condiciones de los niveles de seguridad establecidos por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica", previsión en nuestra opinión innecesaria y hasta absurda, por cuanto también los sistemas que empleen firmas electrónicas longevas, y hasta otros sistemas de identificación y autenticación diferentes de los basados en mecanismos criptográficos, deberán igualmente cumplir las previsiones generales que en materia de seguridad se establecen reglamentariamente.

Parece que también en el caso del repositorio seguro para la conservación de la firma electrónica será aplicable la regla 3ª del epígrafe II.7, que determina que "cada política de firma definirá un servicio para mantener las evidencias de validez de las firmas

[258] Obviamente, es también necesario que el certificado de la entidad que expide los sellos de fecha y hora sea de larga duración, por ejemplo de diez años, y que sólo se emplee el primer año, lo cual permite que los sellos generados duren un mínimo de nueve años.

longevas y gestionar la actualización de las firmas", si bien en este caso resulta de extraordinaria importancia su aplicación, al no existir una especificación técnica de referencia que defina estos aspectos.

Por tanto, cobra mayor valor la parte final de dicha regla, que establece que "dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma como los certificados e informaciones de estado utilizadas en su validación", que realmente deberá describir detalladamente estas cuestiones.

En la regla 4ª del mismo epígrafe II.7 es donde se autoriza que "el almacenamiento de los certificados y las informaciones de estado podrá realizarse […] en un depósito específico: […] b) Si los certificados y las informaciones de estado se almacenan en un depósito específico, se sellarán de forma independiente", al objeto de proteger su integridad y autenticidad para uso probatorio.

Por su parte, la regla 5ª del epígrafe II.7 concreta que "la protección de la firma electrónica frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez, se realizará a través de uno de los siguientes procesos: […] b) Almacenamiento de la firma electrónica en un depósito seguro, garantizando la protección de la firma contra falsificaciones y asegurando la fecha exacta en que se guardó la firma electrónica", resultando a estos efectos muy relevante la determinación de que "las operaciones de fechado se realizarán con marcas de fecha y hora, no siendo necesario su sellado de tiempo", marcas de fecha y hora cuyas medidas de seguridad no se determinan en la Norma Técnica, debiéndose determinar a partir del análisis de riesgos correspondiente, y a tenor de los plazos vigencia legal de la documentación firmada.

4.4.3 Las estrategias de conservación a largo plazo de documentos firmados

Partiendo de lo indicado en las secciones anteriores, 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[259], método por el que en principio apostaría la Norma Técnica analizada. Este método resulta adecuado para proteger una firma unitaria 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[260].

- Adición de sellos de fecha y hora a cada instancia descriptiva de firma electrónica[261]. Este método resulta adecuado para proteger la firma unitaria y las informaciones complementarias y los metadatos correspondientes, especialmente en el escenario de repositorio seguro.

- Adición de sellos de fecha y hora a cada secuencia de firma electrónica[262]. Este

[259] Por objeto de firma electrónica es necesario entender la estructura de datos que contiene los datos de una firma electrónica, típicamente utilizando un formato normalizado, como por ejemplo CAdES, XAdES o PAdES, que se elige en función del formato del documento a firmar (por ejemplo, CAdES sería útil para firmas de documentos binarios, XAdES para la firma de documentos en XML, y PAdES para la firma de documentos en PDF).

[260] Por ejemplo, la respuesta que devuelve una plataforma de validación de firma electrónica (típicamente, un documento XML que informa sobre la firma electrónica verificada) no se puede guardar dentro de la firma electrónica, pero tiene un gran valor evidencial.

[261] Una instancia descriptiva de firma electrónica es un objeto que contiene una firma electrónica y las informaciones y metadatos adicionales que se precisan para su gestión futura.

[262] Una secuencia de firmas electrónicas es una lista ordenada de varias instancias descriptivas de objetos de firmas electrónicas, incluyendo los propios objetos, que se utiliza cuando diversas personas deben firmar un mismo documento, como alternativa a las más complejas “contrafirmas”.

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, sólo 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 (ArchiveTimeStamp) 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[263] 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.

[263] En caso contrario, aún estaría en fase semiactiva o de vigencia.

5 LA CRIPTOGRAFÍA EN LA POLÍTICA DE FIRMA ELECTRÓNICA

La política de firma electrónica se refiere, en su epígrafe III.5 a las "reglas de uso de algoritmos", dentro de las denominadas "reglas comunes", en referencia a los algoritmos criptográficos en que se basa la firma electrónica.

En concreto, la regla 1ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad ordena que "la política de firma especificará las reglas de uso de algoritmos en los diferentes formatos así como la longitud de las claves asociadas a aquéllos de forma proporcional a las necesidades detectadas en los diferentes usos de la firma electrónica, cumpliendo en cualquier caso lo establecido en la NTI de Catálogo de estándares", incluyendo la política criptológica como parte esencial de la política de firma electrónica y de certificados.

Dos son los aspectos de los que debe ocuparse, por tanto, cada concreta política de firma electrónica:

- Establecimiento de las reglas de uso de algoritmos (de resumen, de firma electrónica, según veremos a continuación).

- Determinación de la longitud de las claves empleadas por dichos algoritmos para las operaciones (de resumen, de firma).

Conviene antes, sin embargo, recordar la (escasa) regulación de los criptografía en el régimen general de la LFE, de lo que nos ocupamos a continuación.

5.1 LA CRIPTOGRAFÍA, LAS CIFRAS Y LOS ALGORITMOS CRIPTOGRÁFICOS

La criptografía, motor de sustento de la firma electrónica, 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 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.

La regulación del uso de la criptografía[264] 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[265] tanto a las empresas que producían como a las que trabajaban con criptografía.

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"[266]. La clave aporta la información necesaria para devolver el documento, ara desordenado y por tanto ininteligible, a su estado original, operación que se denomina "descifrar"[267].

---

[264] Cfr. BAKER y HURST, 1998.

[265] 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."

[266] Atención al uso del incorrecto término "encriptar", muy generalizado pero no recogido en el Diccionario de la Real Academia de la Lengua Española.

[267] Atención al uso del también incorrecto término "desencriptar", igualmente generalizado, y tampoco recogido en el Diccionario de la Real Academia de la Lengua Española.

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.

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[268].

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 criptográficos, por tanto, residen en el corazón de la firma electrónica.

El Centro Criptológico Nacional tiene la misión de actuar como entidad de certificación criptológica, evaluando la calidad de dichos algoritmos y, en relación con la firma electrónica y la Administración electrónica, su uso en España, lo cual realiza a través de

[268] Precisamente, la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados prevé, en este epígrafe III.5, un conjunto de reglas de uso de algoritmos aplicables a la firma electrónica, diferenciando entre entornos de seguridad genérica y entornos de alta seguridad.

la publicación de las Guías CCN-STIC-405 y CCN-STIC-807, sobre criptografía, que constituyen excelentes pautas[269] para establecer la política de cada organización en materia criptológica y, más en concreto, para reducir los riesgos de cumplimiento legal.

Uno de los principales inconvenientes de todos los algoritmos es que, debido al tipo de problema matemático en el que se basan, cuya dificultad de resolución es precisamente lo que lo hace seguro, 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 sólo segura mientras tanto el algoritmo como la clave empleada no hayan sido superados por la capacidad de cálculo de un atacante. En términos práctico, 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, como veremos posteriormente.

5.1.1 Los algoritmos de resumen

El algoritmo de resumen, empleado en la firma electrónica, 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

[269] Nótese que la regla 4ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados limita estas recomendaciones únicamente a los entornos de alta seguridad, cuyas dificultades estudiamos posteriormente.

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 2010, de acuerdo con las recomendaciones del Centro Criptológico Nacional para la firma electrónica reconocida (Cfr. Guía CCN-STIC-405).

En nuestra opinión se trata de una política criptológica muy rigurosa, dado que el NIST de los EEUU, aunque considera que el uso de SHA-1 debe considerarse obsoleto por las Agencias Federales a partir de enero de 2011, autoriza su uso hasta diciembre de 2013[270], especialmente debido a que las técnicas de ataque a los algoritmos no han evolucionado como se había previsto, lo cual permite extender las periodos de uso.

Sin embargo, el empleo de SHA-1 en entornos de seguridad genérica está expresamente autorizado por la regla 2 del epígrafe III.5 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados. Asimismo, se trata de un algoritmo también acreditado, con carácter general, por el Centro Criptológico Nacional para su uso en el Esquema Nacional de Seguridad (Cfr. Guia CCN-STIC-807, sección 3.4).

[270] Cfr. NIST Special Publication 800-131ª, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, en http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf (última visita: 10/06/2012).

5.1.2 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.

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, como hemos visto anteriormente. 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.

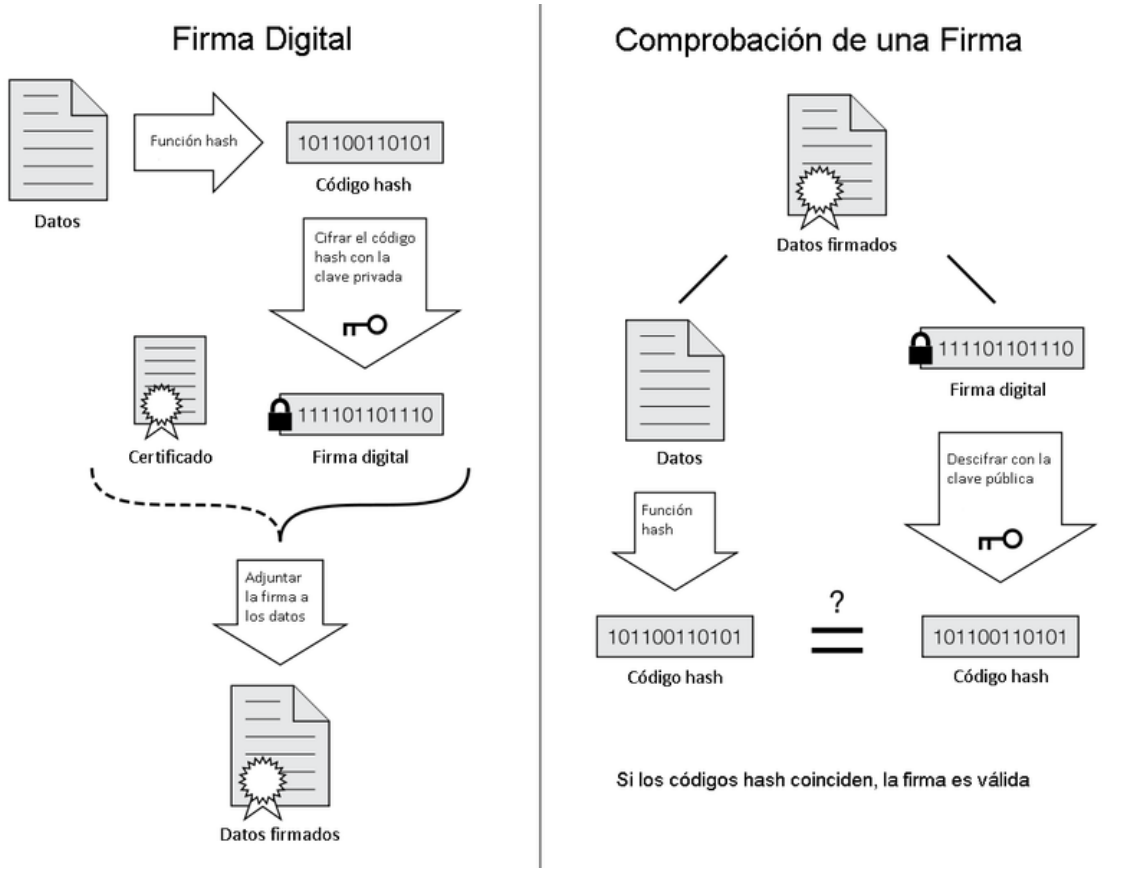
El algoritmo de firma ha de garantizar una serie de condiciones:

- 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.

En general, el algoritmo de firma electrónica funciona de forma conjunta con uno de resumen, por cuestiones de eficiencia computacional, como se puede ver en el

siguiente gráfico[271]:



El algoritmo de firma electrónica que habitualmente se utiliza es RSA con longitud de clave de 1024 bits, si bien el Centro Criptológico Nacional realiza una recomendación fuerte de migración a RSA con longitud de clave de 2048 bits hasta 2010, y a partir de esta fecha, empleo de ECDSA[272] con longitud de claves de 256 bits (Cfr. Guía CCN-STIC-405).

En nuestra opinión se trata de una política criptológica poco justificada, en particular en cuanto a la obligación de abandono del algoritmo RSA. La política del NIST de los EEUU permite a las Agencias Federales perfectamente el empleo de RSA junto a ECDSA o DSA[273], algo que en este caso resulta especialmente relevante, por cuanto impacta

[271] Wikimedia Commons, en http://es.wikipedia.org/wiki/Archivo:Firma_Digital.png (última visita: 15/07/2012).

[272] Algoritmo de firma digital basado en curvas elípticas, actualmente muy poco empleado en España.

[273] Cfr. NIST Special Publication 800-131ª, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, en http://csrc.nist.gov/publications/nistpubs/800-

en los sistemas de firma de los ciudadanos o los profesionales.

Sin embargo, y quizá para mitigar este impacto, el empleo de RSA 1024 bits en entornos de seguridad genérica está expresamente autorizado por la regla 2ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados. Asimismo, se trata de un algoritmo también acreditado, con carácter general, por el Centro Criptológico Nacional para su uso en el Esquema Nacional de Seguridad (Cfr. Guía CCN-STIC-807, sección 3.3).

Por su parte, el empleo de RSA 2048 bits y ECDSA 256 bits aplicaría al uso de la firma electrónica en entornos de alta seguridad, de acuerdo con la regla 4ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados.

5.2 LAS CLAVES CRIPTOGRÁFICAS

Las claves criptográficas son los elementos numéricos que forman una cifra criptográfica, y que 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, o de poder acceder a sus datos secretos, pudiendo afectar, además, a la eficacia jurídica de la actuación realizada.

Entre nosotros, LINARES GIL, 2010: p. 426; 2012: pp. 482 y ss. se ha referido a las claves de generación y de verificación de firma como el corazón del sistema de firma digital criticando el olvido a las mismas en las definiciones contenidas tanto en la LAE como en la LUTICAJ.

131A/sp800-131A.pdf (última visita: 10/06/2012).

La LFE regula las claves criptográficas, a las que otorga 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[274].

- 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.

El conjunto más importante de medidas de seguridad en materia, consecuentemente, 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.

[274] Excepto cuando los datos de creación de firma sean generados en un hardware específico, y posteriormente exportados al dispositivo seguro de creación de firma, posibilidad expresamente admitida en las especificaciones técnicas europeas (cfr. CEN CWA 14167 y 14169).

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.

Sin embargo, la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración no se ha ocupado establecer prácticamente ninguna norma en relación con las claves ni los dispositivos de creación de firma. Sólo la regla 1ª del epígrafe III.5 contiene una somera referencia a la necesidad de establecer una longitud suficiente de las claves empleadas.

Esta aproximación nos parece criticable en relación, al menos, con los sistemas de firma electrónica basados en Código Seguro de Verificación, que con carácter general se basan en determinados algoritmos criptográficos similares a los empleados para la autenticación y la firma electrónica.

En concreto, diversos sistemas de Código Seguro de Verificación se basan en algoritmos Keyed Hash MAC, y quizá hubiese sido interesante establecer algunas reglas de interoperabilidad[275] para el intercambio de documentos autenticados mediante este mecanismo.

Más criticable nos resulta la ausencia de toda regulación, ya avanzada anteriormente[276], a sistemas de firma electrónica avanzada basados en claves criptográficas de consulta en línea que, por tanto, no hacen uso de certificados digitales, como por ejemplo XKMS.

[275] Una posible explicación a esta carencia la podemos encontrar en que estos mecanismos se verifican en la sede electrónica del organismo emisor, por lo que se requieren un menor nivel de normalización en su empleo.

[276] Cfr. la sección 2.1.3 de este trabajo.

5.2.1 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, sólo 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 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.

La Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración no se ha ocupado de establecer normas directamente relacionadas con la interoperabilidad de las claves, seguramente por considerar que dichas reglas se deduce de forma implícita a partir de las reglas aplicables a los algoritmos, lo cual sólo es parcialmente cierto.

5.2.2 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.

De nuevo, la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración ha evitado establecer normas directamente relacionadas con la correlación de las claves, seguramente por considerar que dichas reglas se deduce de forma implícita a partir de las reglas aplicables a los algoritmos, lo cual sólo es parcialmente cierto.

5.2.3 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[277], mientras que la clave privada de un prestador de servicios de certificación habitualmente tiene una longitud de 2048 bits[278].

En este sentido, la regla 1ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración obliga a determinar, en cada concreta política de firma electrónica, "la longitud de las claves asociadas a aquéllos de forma proporcional a las necesidades detectadas en los diferentes usos de la firma electrónica", en principio a partir de las recomendaciones que pueda dictar del Centro Criptológico Nacional para la firma electrónica, en su condición de autoridad competente en materia de cifra, según hemos visto anteriormente[279].

5.2.4 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

[277] En este sentido, valga como ejemplo que la Agencia Estatal de Administración Tributaria admite certificados cuya clave de usuario tenga una longitud de al menos 512 bits.

[278] La clave de la autoridad de certificación raíz debería tener, al menos, 4096 bits, al efecto de proteger las claves de las autoridades de certificación subordinadas durante un periodo largo de tiempo (cfr. Guía CCN-STIC-405).

[279] Cfr. las secciones 5.1.1 y 5.1.2 de este trabajo.

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.

Tampoco en este caso ha establecido la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración reglas respecto de la generación de las claves, y posiblemente sea cierto que no se trata de una cuestión de interoperabilidad, sino de seguridad y confianza, pero tampoco lo es la longitud de claves y en cambio sí se ha tratado dicho aspecto.

5.2.5 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".

BAUZÁ MARTORELL, 2002: pp. 65 y ss. se ha referido a los problemas que, a su juicio, pueden derivarse de la que denomina "escindibilidad" de la firma electrónica, indicando que "sólo la seguridad del par de claves a través de un dispositivo de identificación biométrica puede resultar idóneo para asegurar que el signatario de un documento mediante una clave es titular de la misma, sin perjuicio de que la huella biométrica exclusivamente garantice el acceso al sistema informático, de manera que en modo alguno acreditará que el uso posterior al acceso es el que dice ser", crítica que no podemos compartir, dado que conduce a la imposibilidad lógica de considerar

la existencia de ningún sistema técnico como idóneo para producir el equivalente de una firma escrita, pero que muestra perfectamente la preocupación jurídica por las posibles presunciones en favor de la veracidad de la firma electrónica y la imputación de las consecuencias jurídicas de acto al autor supuesto.

A la protección de la clave hace referencia la propia definición de la firma electrónica avanzada, cuando indica que ésta 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).

Tampoco en este caso ha establecido la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración reglas respecto de la protección de las claves, y de nuevo es cierto que no se trata de una cuestión de interoperabilidad, sino de seguridad y confianza, a pesar de lo cual nada obsta a que la política de firma electrónica establezca alguna norma al respecto, ya que este instrumento no es exclusivamente de interoperabilidad, sino que vela también por la confianza en las firmas electrónicas generadas.

5.2.6 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[280] – se puede acceder a los datos de creación

[280] Obviamente, no se puede hablar en puridad de delegación ninguna, dado que la firma se imputará al firmante aparente.

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; son 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.

Una vez más, la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración ha optado por no establecer reglas respecto de los datos de activación de firma, sin perjuicio de que la política de firma electrónica pueda establecer alguna norma al respecto, ya que este instrumento vela también por la confianza en las firmas electrónicas generadas.

5.3 LOS DISPOSITIVOS DE FIRMA ELECTRÓNICA

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; definición que conecta la creación 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[281] se han convertido en los

[281] Se trata de aplicaciones o software de amplio uso instalado en los sistemas operativos más habituales, de acuerdo con dos especificaciones técnicas de programación (CSP en entorno Microsoft y PKCS11 en todos los entornos).

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[282].

La Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración establece algunas reglas que afectan al funcionamiento de los dispositivos de creación y de validación de firma electrónica, que hemos estudiado en sede de procesos de firma electrónica[283].

5.3.1 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 sólo 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 éste se muestre al firmante antes del proceso de firma.

---

[282] Aunque algunas aplicaciones así los consideran: en concreto, la Agencia Estatal de Administración Tributaria ha reconocido que, a los efectos de sus procedimientos administrativos, se considera que los proveedores de servicios criptográficos son dispositivos seguros, algo que nos parece absolutamente criticable, por generar una cierta confusión en el mercado.

[283] Cfr. la sección 4.3.1 de este trabajo.

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[284] 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 información, para dispositivos seguros de creación de firma electrónica; es decir, 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 profesionales colegiados, por citar dos ejemplos.

Por su parte, la especificación técnica CEN CWA 14170 ofrece un conjunto de medidas de seguridad funcional aplicables a las aplicaciones y programas que funcionan conjuntamente con dispositivos seguros de creación de firma electrónica (aplicaciones 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[285] 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

[284] Publicada en España por AENOR como UNE-CWA 14169:2005.

[285] Dicho procedimiento es voluntario y su relevancia, como indica MARTÍNEZ NADAL, 2009: p. 494, básicamente comercial, en el sentido de que el fabricante o importador que haya obtenido la correspondiente certificación aparecerá en el mercado con una apariencia de mayor calidad, pudiendo servir para dar una orientación y una mayor seguridad a los usuarios a la hora de elegir su producto de firma electrónica.

web del Portal de Criterios Comunes[286], lo cual facilita la verificación por el firmante del cumplimiento de la legislación de firma electrónica por parte de estos productos[287].

Aunque la Norma Técnica de Interoperabilidad no se refiere de forma expresa a estos dispositivos, las reglas aplicables al proceso de creación de firma electrónica que hemos analizado anteriormente[288] resultan plenamente aplicables a los mismos, por lo que deberán ser tomadas en consideración en el momento de la adquisición de los mismos. Por otra parte, también el RDENS se refiere a estos dispositivos en relación con la firma electrónica, siendo su uso recomendable en sistemas de nivel medio de seguridad, y obligatorio en sistemas de nivel alto.

5.3.2 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, olvidándose el legislador de 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, siempre que sea técnicamente

---

[286] Common Criteria Portal, accesible en http://www.commoncriteriaportal.org/products/ (última visita: 14/06/2012).

[287] Habitualmente será el prestador de servicios de certificación el que asuma esta verificación, dado que adquiere para el firmante el dispositivo, lo personaliza y lo entrega debidamente operativo.

[288] Cfr. la sección 4.3 de este trabajo.

posible, concepto jurídico indeterminado que hay que resolver con 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.

Aunque la Norma Técnica de Interoperabilidad no se refiere de forma expresa a estos dispositivos, las reglas aplicables al proceso de validación de firma electrónica que hemos analizado anteriormente[289] resultan plenamente aplicables a los mismos, por lo que deberán ser tomadas en consideración en el momento de su adquisición, configuración y operación.

Específicamente, las plataformas de verificación de firma electrónica y certificados a las que aluden los artículos 21.3 de la LAE y 22.2 de la LUTICAJ, y el artículo 20 del RDENI son dispositivos pertenecientes a esta categoría.

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.

5.4 CRÍTICA A LA APLICACIÓN DE LA POLÍTICA CRIPTOLÓGICA DE LA NORMA TÉCNICA DE INTEROPERABILIDAD

Como hemos avanzado en las secciones anteriores, en el epígrafe III.5 de la Norma Técnica de Interoperabilidad se establecen dos categorías de seguridad a efectos de la determinación de los algoritmos criptográficos.

En concreto, la regla 2ª establece que "para los entornos de seguridad genérica[290] se tomará la referencia a la URN (Uniform Resource Name) en la que se publican las

[289] Cfr. la sección 4.3.1.4 de este trabajo.

[290] El subrayado es nuestro.

funciones hash y los algoritmos de firma utilizados por las especificaciones XAdES, CAdES y PAdES, como formatos de firma adoptados, de acuerdo con las especificaciones técnicas ETSI TS 102 176-1, «Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms». Todo ello sin perjuicio de los criterios que al respecto se establezcan atendiendo al Real Decreto 3/2010, de 8 de enero".

Mientras que la regla 3ª indica que "se admitirán como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en los estándares XML-DSig (XML Digital Signature) y CMS (Cryptographic Message Syntax)".

Finalmente, la regla 4ª determina que "para los entornos de alta seguridad[291], de acuerdo con el criterio del Centro Criptológico Nacional (CCN) serán de aplicación las recomendaciones revisadas de la CCN-STIC 405 así como en la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía".

Esta determinación no está precisamente exenta de problemas, tanto debido a la oscuridad del precepto, cuanto por su indeterminación. En efecto, resulta difícil dilucidar las condiciones de aplicabilidad de ambos niveles de seguridad, debido a la ausencia de mayores indicaciones en la Norma Técnica de Interoperabilidad.

Del análisis de las especificaciones técnicas mencionadas en la regla 2ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad[292] se deduce la posibilidad de emplear cualquiera de los algoritmos allí identificados para la producción de firmas electrónicas avanzadas y reconocidas, por lo que resulta que el nivel genérico de seguridad cubre, en principio, todos los casos de uso de firma electrónica.

---

[291] El subrayado es nuestro.

[292] En concreto, ETSI TS 102 176-1 es un trabajo que se realizó en el ETSI, bajo la dirección del EESSI, para disponer de un referente referido a qué algoritmos se podían emplear precisamente para la producción de la firma electrónica reconocida. En la actualidad, sin embargo, se trata de un documento ciertamente desfasado, ya que los trabajos de actualización de este documento han sido encargados a la Red Europea de Excelencia en Criptología II, que publica versiones actualizadas de las recomendaciones, en su página web: http://www.ecrypt.eu.org/documents/D.SPA.17.pdf (última visita: 3/09/2012).

De mayor ayuda resulta la referencia a "los criterios que al respecto se establezcan atendiendo al Real Decreto 3/2010, de 8 de enero", que aprueba, como sabemos, el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, estableciendo tres categorías de seguridad para los sistemas de información[293].

Una vez determinado el nivel de seguridad requerido en las dimensiones de autenticidad e integridad, el anexo II determina la aplicación de las siguientes reglas criptográficas, contenidas en el epígrafe 5.7.4:

- En el nivel bajo se empleará cualquier medio de firma electrónica de los previstos en la legislación vigente, por lo que, en principio, no se establecería restricción ninguna en cuanto a los algoritmos a emplear.

- En el nivel medio, se establece que los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada, y que en todo caso se emplearán algoritmos acreditados por el Centro Criptológico Nacional[294].

- En el nivel alto, se indica que se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en el nivel medio, además del empleo de dispositivos seguros de creación de firma y, preferentemente, de productos certificados.

El ámbito de aplicación, en consecuencia, del nivel genérico de seguridad previsto en la Norma Técnica de Interoperabilidad coincidiría, por tanto, con el nivel bajo de seguridad del Esquema Nacional de Seguridad, y también con el nivel medio de éste último, siempre que los algoritmos fueran acreditados por el Centro Criptológico Nacional.

Sin embargo, hemos podido ver la que la regla 3ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad establece la validez de los algoritmos indicados en los estándares XMLDSig y CMS deben ser necesariamente admitidos como válidos, lo cual resulta

[293] Cfr. la sección 4.3.2 de este trabajo.

[294] Los algoritmos acreditados, y sus normas de uso, se encuentran en la Guía CCN-STIC-807.

contradictorio con la regla 2ª, especialmente cuando se contrasta con lo establecido en el Esquema Nacional de Seguridad.

Se puede salvar esta aparente contradicción entendiendo que la regla 2ª del epígrafe III.5 se dirige a regular la creación de la firma electrónica, mientras que la regla 3ª se orienta a regular la admisión y verificación de la firma electrónica, pero ciertamente nos resulta criticable tan defectuosa redacción.

Y si difícil resulta determinar el alcance del "entorno de seguridad genérica", aún resulta más complejo determinar el alcance del "entorno de alta seguridad" referido en la regla 4ª del epígrafe III.5.

Una posibilidad razonable sería hacer coincidir este entorno de seguridad alta con el nivel de seguridad alto del RDENS, de forma que los algoritmos acreditados serían utilizados en los dispositivos de firma, en su caso, certificados en seguridad, pero hay que reconocer que nada[295] en la documentación del Centro Criptológico Nacional permite establecer una equiparación clara entre ambos niveles, especialmente en relación con las muy estrictas indicaciones de la Guía CCN-STIC-405 a que ya nos hemos referido.

En otro orden de cosas, en nuestra opinión se podría haber tratado más ampliamente el uso de la criptografía en la Norma Técnica de Interoperabilidad, sin perjuicio de la posibilidad de realizarlo estas determinaciones en cada concreta política de firma electrónica, como autoriza la regla 5ª del citado epígrafe III.5, que dispone que "la definición de usos de algoritmos podrá contemplar diferentes posibilidades según las necesidades en cada caso", previsión claramente insuficiente.

[295] En este sentido, las recomendaciones de la Guía CCN-STIC-807 para nivel alto de seguridad son menos estrictas que las recomendaciones de la Guía CCN-STIC-405, lo cual impide establecer un ámbito adecuado de aplicación de la última guía.

6 LOS CERTIFICADOS ELECTRÓNICOS EN LA POLÍTICA DE FIRMA ELECTRÓNICA

La Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración establece, como resulta natural, diversas reglas aplicables a los certificados electrónicos, en el epígrafe IV.1, titulado "Reglas de confianza para los certificados electrónicos", que procede analizar con cierto detalle.

6.1 EL RÉGIMEN JURÍDICO GENERAL DE LOS CERTIFICADOS ELECTRÓNICOS

Con carácter general, un certificado electrónico es, sencillamente, un documento electrónico firmado[296] 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 cierta cantidad de posibles certificados, de los cuales sólo una pequeña parte ha sido regulada legalmente, y con la finalidad de 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[297], al cual

[296] Por el prestador de servicios de certificación que lo expide, como garantía de seguridad y confianza en la mismo, de acuerdo con las obligaciones legales y, en su caso, convencionales, que resulten aplicables.

[297] Como veremos, el derecho de admisión de la firma electrónica se ha construido sobre el certificado electrónico reconocido, pasando a ser uno de los aspectos tratados en la política de firma electrónica y de certificados.

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[298] (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.

Los certificados se pueden clasificar de acuerdo con diversos criterios, entre los cuales tenemos los certificados de clave pública o certificados de atributos; los certificados de autoridad de certificación o de usuario final; y los certificados de firma electrónica o de cifrado.

En esta sección presentamos, también, diferentes tipos de certificados habitualmente empleados en el procedimiento administrativo o judicial, por su relevancia en el contexto de la política de firma electrónica.

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[299].

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, y se denomina "de claves públicas" porque las operaciones de firma y cifrado requieren como elemento fundamental la publicación y la distribución de las

[298] Internet Engineering Task Force, una comunidad internacional de diseñadores, operadores, fabricantes e investigadores sobre las redes, que desarrolla las principales especificaciones técnicas de Internet. Cfr. http://www.ietf.org/rfc/rfc3935.txt (última visita: 15/06/2012).

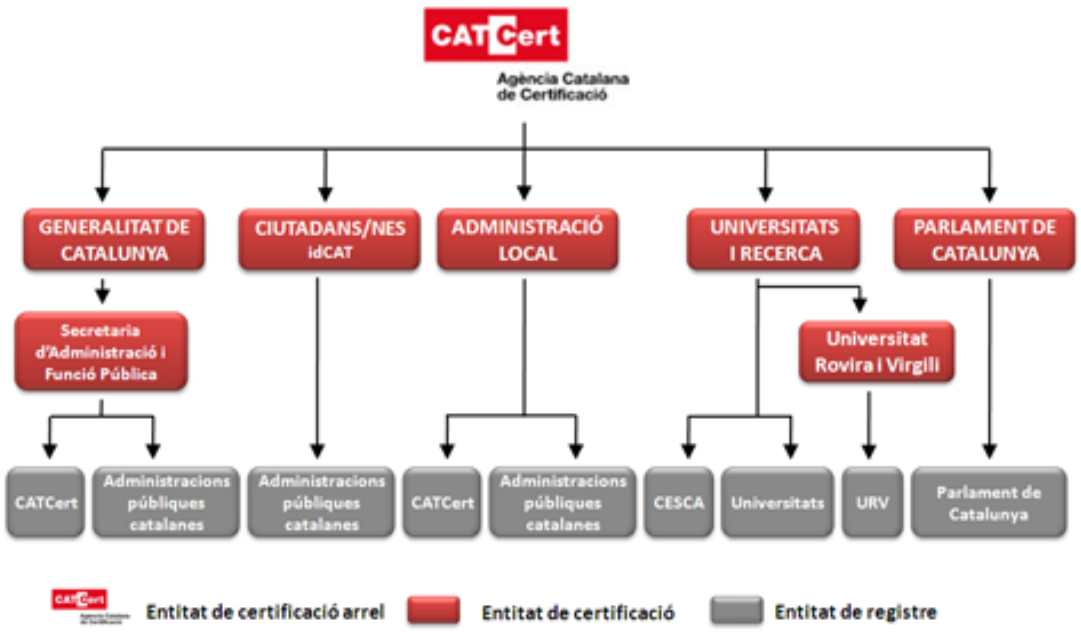
[299] Para una descripción técnica completa de las infraestructuras de clave pública, cfr. ADAMS y LLOYD, 1999 y FORD y BAUM, 1997; así como, en general, los trabajos del grupo PKIX del IETF, en

claves públicas de los usuarios[300] de los servicios, que suelen distribuirse 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 éstas y los usuarios determinan el modelo de confianza de la infraestructura de claves públicas.

El modelo más ampliamente implantado de infraestructura de certificación es el jerárquico, en el que una autoridad de certificación actúa como principal, o raíz, de una cierta comunidad de usuarios de certificados, como se puede ver en el siguiente gráfico, correspondiente a la Agència Catalana de Certificació – CATCert:



http://datatracker.ietf.org/wg/pkix/charter/ (última visita: 15/06/2012).

[300] Recuérdese que, como hemos visto en la sección 5.2 de este trabajo, la clave pública permite verificar las firmas producidas empleando la clave privada, cuyo secreto es imprescindible para la

Como se puede apreciar, debajo de la autoridad de certificación principal, este prestador ha desplegado otras autoridades de certificación intermedias, al objeto de expedir certificados para diversas comunidades de usuarios[301].

En toda infraestructura de clave pública se diferencia entre dos tipos de certificados:

- El certificado de autoridad de certificación es un certificado de clave pública expedido a un componente técnico de toda infraestructura de servicios de certificación, que se denomina autoridad de certificación, y que es empleado por el prestador de servicios de certificación para la expedición de los certificados[302].

  Dicho componente técnico debe recibir su propio certificado, con la finalidad de establecer un modelo de confianza que nos permita comprobar y utilizar los certificados que expide dicha autoridad de certificación (actividad que legalmente, como también veremos, se denomina "prestación de servicios de certificación").

- El certificado de usuario final, que es todo aquel certificado, de clave pública o de atributos, expedido por una autoridad de certificación para firmar, verificar, cifrar o descifrar documentos por parte de usuarios finales del servicio (frecuentemente consumidores). La única restricción que deben tener, en todo caso, es la prohibición de expedir otros certificados, dado que en este caso

---

imputación de la condición de firmante.

[301] Como indica la Política de Certificación de la Agència Catalana de Certificació, "la Agencia Catalana de Certificació se constituye en la entidad principal del sistema público catalán de certificación que regula la emisión y la gestión de los certificados que se emitan para las instituciones de autogobierno de Catalunya, las instituciones que integran el mundo local, y el resto de entidades públicas y privadas que integran el sector público catalán; así como la admisión y el uso de los certificados emitidos a ciudadanos y empresas por otros prestadores de servicios de certificación y que soliciten la correspondiente clasificación. Estas instituciones emitirán certificados por medio de una infraestructura técnica proporcionada por CATCert, denominada "jerarquía pública de certificación de Catalunya", y podrán admitir y utilizar certificados de otros prestadores mediante los servicios de clasificación y validación de CATCert".

[302] Aunque, en general, se suele considerar que "autoridad de certificación" y "prestador de servicios de certificación" son sinónimos, en realidad los prestadores de servicios de certificación pueden no expedir certificados, sino ofrecer otros servicios, como el sellado de fecha y hora.

serían certificados de autoridad de certificación, y no de usuario final.

6.1.1 Certificado de clave pública o de atributos

El certificado de clave pública contiene la clave pública de una persona o entidad identificada, que dispone de la clave privada correspondiente para firmar documentos, autenticarse ante terceros o descifrar documentos que hayan sido cifrados por terceros utilizando su clave pública.

En función de estas finalidades, especialmente cuando la misma persona recibe diferentes certificados – uno para identificarse y firmar, y otro para descifrar – hablamos de certificados de identidad, certificados de firma electrónica y certificados de cifrado.

Los certificados de atributos, por otra parte, no tienen ninguna clave pública, sino sencillamente la identificación de la persona – generalmente mediante una referencia a su certificado de clave pública – y un conjunto de atributos.

Estos certificados se utilizan para certificar información muy variable en el tiempo, o que no se desea o no se puede incluir en el certificado de clave pública[303].

Los certificados de clave pública y los de atributos han sido definidos por la Recomendación ITU-T X.509, que también ha sido publicada como Norma Internacional ISO/IEC 9594-8, y perfilados posteriormente por el IETF, para su uso en la red Internet y otras redes basadas en los protocolos TCP/IP.

Habitualmente, el certificado de clave pública también contiene otras informaciones personales, como por ejemplo el cargo administrativo o la condición de profesional colegiado del titular del certificado. En este caso, se denominan certificados de clave pública con atributos o, sencillamente, certificados con atributos.

Veremos, a continuación, dos casos muy relevantes de uso de certificados de clave

[303] Los certificados de atributos precisamente fueron diseñados para poder certificar informaciones de efímera vida, incluso de minutos.

pública con atributos, de posible uso en el procedimiento electrónico, como son los certificados corporativos y los de representación.

6.1.1.1 Certificado individual y certificado 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; es el modelo de certificado sobre el 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.

Estos certificados, que se pueden encuadrar en los "certificados de clave pública con atributos" a los que nos hemos referido *supra*, se están desarrollando de forma satisfactoria en el mercado, por el valor añadido que representan y su semántica permite aprovechamientos potencialmente muy interesantes.

En función de la semántica de los atributos que contienen, estos certificados corporativos se pueden adjetivar de la siguiente forma:

- Certificados de órgano[304].
- Certificados de empleado[305].
- Certificados de profesional, en su caso colegiado[306].
- Certificados de representación[307].

6.1.1.2 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, deberán 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[308], cuyo uso permitiría la simplificación del

[304] Por ejemplo, la inclusión de un atributo a una certificado personal corporativo donde se indique la condición del firmante de administrador único de una sociedad de capital, o la condición de alcalde (cfr. sección 6.2.1.1 de este trabajo para más información de estos certificados en el ámbito público).

[305] Empleados, con una cierta profusión, por ejemplo en el ámbito de la facturación electrónica, y definidos específicamente para el ámbito de la Administración electrónica (cfr. sección 6.2.1.2 de este trabajo).

[306] A título de ejemplo, el artículo 6.2.d) de la LUTICAJ condiciona el derecho de uso de los sistemas de firma electrónica de los profesionales en el ámbito de la justicia, a que los mismos les identifiquen de forma unívoca como profesional para cualquier trámite electrónico con la Administración en los términos establecidos por las leyes procesales.

[307] A estos certificados dedicamos la siguiente sección.

[308] La doctrina ha analizado con preocupación el problema de la concordancia entre el atributo –dinámico – de la representación indicado en el certificado y el correspondiente Registro público, en particular en el caso del Registro Mercantil (cfr. MARTÍNEZ NADAL, 2009: pp. 220 y ss.). Cfr. VALERO TORRIJOS, 2007: p. 101, quien considera que este tipo de certificado tampoco podría ser empleado cuando la

procedimiento, administrativo o judicial, en el cual dejaría de resultar necesaria la aportación del clásico apoderamiento[309].

El artículo 11.4 de la LFE determina que el certificado reconocido de 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 hacer 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.

6.1.2 Certificado de firma electrónica, de identificación o de cifrado

Como se ha indicado en la sección anterior, los certificados de clave pública de usuario final pueden ser de firma electrónica, de identificación o de cifrado.

---

normativa exija la intervención preceptiva de fedatario público, conclusión que sólo podemos compartir si entendemos que se refiere a la intervención del acto, no al otorgamiento del poder de representación, que la LFE ha previsto como requisito precisamente para la expedición del certificado de representante.

[309] No parece ser, sin embargo, ésta la orientación del legislador de la LUTICAJ en el caso de la representación procesal, dado el tenor del artículo 40.1 de la ley, que obliga a la aportación de copia electrónica del poder notarial de representación o verificación directa, en caso de impugnación, mediante los sistemas de la Agencia Notarial de Certificación. Caso distinto podría darse, en nuestra opinión, en los casos en que el ciudadano (a través de su representante) actúe directamente sin asistencia letrada ni representación procesal, ex. artículo 36.1 de la LUTICAJ, en relación con los artículos 6, 7 y 23.2 de la LEC; posibilidad que parece interesante al menos en el caso de la petición inicial del procedimiento monitorio (artículo 814 de la LEC).

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. Por su parte, el certificado de firma electrónica y el de identificación son idénticos excepto en el uso autorizado de la clave, que en el primer caso se refiere a la actuación formalizada documentalmente, y en el segundo, únicamente la autenticación.

Estos tres certificados 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, aún en caso de pérdida de la clave privada, se pueden aún 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.

Por otra parte, la mezcla del certificado de identificación con el de firma puede afectar a la calidad de ciertas firmas generadas, porque las aplicaciones de autenticación no suelen implementar controles suficientes para garantizar la declaración de voluntad.

6.1.3 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 certificado de otras funcionalidad (como el cifrado), que por tanto quedan sin regulación directa[310].

Este primer tipo de certificado de firma electrónica se denomina "ordinario" para diferenciarlo del certificado "reconocido" – una traducción ambigua, por cierto, 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"[311].

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, según hemos expuesto anteriormente. Es curioso ver como 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[312].

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; mientras que, por su menor importancia,

---

[310] En la práctica de la mayoría de prestadores de servicios de certificación, sin embargo, se puede observar la aplicación de las reglas de los certificados de firma electrónica (en especial de los certificados reconocidos) a los restantes tipos de certificados que expiden. Asimismo, tanto en la LAECSP como en la LUTICAJ se indica que el sello de actuación automatizada se basa en un certificado que reúna los requisitos exigidos en la legislación de firma electrónica, referencia insuficiente claramente, dada la diferencia de regulación entre el certificado ordinario y el certificado reconocido. Es de suponer que el legislador se esté refiriendo a que los sellos de actuación automatizada deban cumplir lo previsto para los certificados reconocidos, con las necesarias adaptaciones.

[311] Dado que se trata sólo de un tipo específico de certificado, cualificado por el uso que hace del mismo una persona física para la producción de una firma electrónica idónea para imputarle sus declaraciones de voluntad.

[312] Esta situación, en nuestra opinión, se ha agravado con la LAECSP y la LUTICAJ, que remiten a la LFE aspectos de certificados notablemente diferentes a los regulados en la citada ley.

la regulación del certificado ordinario es también menor: no se regula el contenido, y sólo 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[313] o mediante un seudónimo que conste como tal de manera inequívoca[314] 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.

[313] En el ámbito de la Administración electrónica, desde la Orden HAC/1181/2003, de 12 de mayo, se exige el Número de Identificación Fiscal del firmante, condición de previsible extensión al ámbito del procedimiento judicial.

[314] Como veremos, suele ser una condición adicional exigible en el ámbito del procedimiento administrativo que los certificados no identifiquen al firmante mediante seudónimo, restricción que también parece razonable en el ámbito del procedimiento judicial, al menos en el caso de los ciudadanos y los profesionales que les representan, pero que podría resultar exorbitante en otros casos (por ejemplo, psicólogos de prisiones que firman bajo Número de Personal los informes de cambio de grado penitenciario, que se incorporan al correspondiente expediente penitenciario).

- Los límites de uso del certificado, si se prevén[315].

- 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 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.

6.1.4 Certificado de persona física, de persona jurídica o de entidad sin personalidad

El certificado de persona física es el que se expide a un usuario individual, que se denomina suscriptor del certificado, que será el firmante – en certificados de clave pública de firma – o el que descifre los documentos protegidos con su clave pública – en certificados de cifrado.

El certificado de persona jurídica – que no existe en la DFE – no se define en la LFE, pero a partir del artículo 7 de la Ley, que lo regula, podemos describirlo como el que permite imputar la calidad de autor de los documentos directamente a la persona jurídica (apartado 4), siempre que estos documentos hayan sido firmado dentro de una relación con las Administraciones públicas o dentro del giro o tráfico ordinario de la persona jurídica (apartado 3).

Parece que las aplicaciones del certificado de persona jurídica tengan más que ver con la producción de documentos originales imputables a la entidad que con la firma escrita del apoderado de la entidad[316].

---

[315] El establecimiento de límites constituye hoy uno de los principales retos en el uso de la firma electrónica, debido a la ausencia de estándares que indiquen cómo representarlos y procesarlos informáticamente, por lo que normalmente la Administración no admite estos certificados, o lo hace bajo declaración del firmante referida a que su certificado no contiene ningún límite incompatible con el uso que pretende realizar (por ejemplo, presentar electrónicamente un escrito).

[316] En este sentido, se trata de una figura que ha generado controversia (A título de ejemplo, MARTÍNEZ

El certificado de persona jurídica, sin embargo, realmente se expide con la intervención necesaria de una persona física, porque es necesario que lo solicite, en nombre de la persona jurídica, su administrador, representante legal o voluntario con poder suficiente a estos efectos (apartado 1), que se denomina "custodio"[317].

Las aplicaciones del certificado de persona jurídica tienen más que ver con la producción de documentos originales imputables a la entidad que con la firma escrita del representante legal o voluntario de la persona jurídica, posibilidad que obliga a replantear la necesidad de la representación en la relación electrónica entre las personas jurídicas y las Administraciones Públicas, ya que legalmente es la persona jurídica la que directamente actúa.

Además, el certificado de persona jurídica no podrá afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica (apartado 1 *in fine*), previsión que genera bastantes problemas jurídicos para delimitar qué actos podrían eventualmente quedar excluidos de la "firma de persona jurídica" en la relación electrónica con la Administración.

En nuestra opinión, se debe considerar que esta previsión legal realmente señala que precisamente en la actuación electrónica de la persona jurídica mediante su firma electrónica no existe representación, por ser innecesaria, de forma que en general será

NADAL, 2009: pp. 147 y ss.; ORTEGA DÍAZ: 2008, pp. 282 y ss.) y que en la Propuesta de Reglamento europeo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior se regule de forma radicalmente diferente a la norma española, denominándolo sello electrónico, y otorgándole un régimen jurídico y efectos jurídicos propios. Cfr. COM (2012) 238 final, en especial artículo 28 y ss.

[317] El custodio de un certificado de persona jurídica es la persona física solicitante de un certificado de persona jurídica, que dispone de un dispositivo de firma electrónica y que, por tanto, lo utiliza para producir firmas electrónicas.

El custodio es un administrador, representante legal o voluntario de la persona jurídica, con poderes suficientes para solicitar el certificado de persona jurídica (no, en cambio, para los actos realizados con el certificado, que se imputan a la persona jurídica por efecto de la ley, sin necesidad de poder).

El custodio ha de utilizar el certificado de la persona jurídica dentro de sus límites. En otro caso, el responsable de los actos podría ser el custodio, a título personal.

Por este motivo, el custodio dispone del derecho (y del deber) de revocación del certificado. Adicionalmente, hay que decir que las circunstancias que afecten al custodio afectarán a la vida del certificado de persona jurídica.

posible que actúe directamente la empresa con su firma de persona jurídica[318] o, indistintamente, que actúe un representante mediante un certificado de persona física, en este segundo caso acreditando su representación de forma suficiente.

La regulación del certificado de persona jurídica no se aplica ni a los certificados de las entidades de certificación de firma electrónica[319] ni a los certificados emitidos a favor de las Administraciones Públicas, que se regirán por su normativa específica[320]; a saber, por lo que se refiere a éstas últimas, la LAE y sus correspondientes reglamentos de desarrollo.

Por su parte, la disposición adicional tercera de la LFE prevé la posibilidad que se puedan "expedir certificados a las entidades sin personalidad jurídica propia a las que se refiere el artículo 33 de la Ley General Tributaria, en los términos que determine el Ministro de Hacienda".

Estos certificados sólo podían utilizarse en el ámbito tributario, hasta que el artículo 15.3 de la LAE ha establecido, como novedad en relación a la LFE, que "los certificados electrónicos expedidos a entidades sin personalidad jurídica, previstos en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica podrán ser admitidos por las Administraciones Públicas en los términos que éstas determinen".

Actualmente, la emisión de certificados para entidades sin personalidad jurídica se regula por Orden EHA/3256/2004, de 30 de septiembre, por la que se establecen los términos en los que podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 35.4 de la Ley General Tributaria.

Dicha Orden aplica a las entidades sin personalidad jurídica normas análogas a las

---

[318] Estamos, sin embargo, de acuerdo con VALERO TORRIJOS, 2007: p. 101, en que esta posibilidad se encuentra limitada a los casos donde no exista una norma legal que exija la intervención preceptiva de fedatario público, en cuyo caso "sólo podría admitirse que el documento acreditativo de la representación estuviera firmado digitalmente por un notario o registrador mercantil, quienes habrán de utilizar los certificados expedidos por el prestador autorizado al efecto".

[319] Así lo dispone el artículo 7.5 de la LFE.

[320] Artículo 7.6 de la LFE. Cfr. la sección 6.2.2 de este trabajo, donde presentamos el certificado de sello electrónico de Administración Pública, órgano o entidad de derecho público.

aplicables para los certificados de personas jurídicas, aunque con especialidades, en particular en cuanto al procedimiento de registro, con la finalidad de asegurar que sólo un representante legal o voluntario de la entidad sin personalidad - que actuará como custodio - recibe el certificado.

6.2 UNA REGULACIÓN PROPIA PARA LOS CERTIFICADOS DE LA ADMINISTRACIÓN

La LAE y la LUTICAJ han establecido reglas específicas en cuanto a los certificados electrónicos que puede emplear para la firma electrónica, que presentamos a continuación.

6.2.1 Los certificados corporativos en la Administración

La LAE y la LUTICAJ consideran los certificados corporativos de forma implícita, en el artículo 19 de la LAE, referido a la firma electrónica del personal al servicio de la Administración Pública, así como en el artículo 21 de la LUTICAJ, al tratar la firma electrónica de magistrados, jueces, secretarios judiciales, fiscales, abogados del estado y funcionarios al servicio de la Administración de Justicia y otros entes públicos.

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[321] a su personal de firma electrónica, con los efectos que deriven del tipo de firma que se atribuya y en relación al trámite o procedimiento de que se trate, valorándose igualmente si nos movemos

[321] LINARES GIL, 2010: pp. 434 y ss. critica el empleo de la forma potestativa del verbo, ya que en su opinión "la autenticación de la actividad administrativa es algo inexorable y el medio de lograrlo cuando se trata de documentos electrónicos es precisamente la firma electrónica. […] Sin firma electrónica de los empleados públicos no es posible la identificación ni autenticación del ejercicio de las competencias de la Administración Pública electrónica", crítica que compartimos plenamente.

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.

Examinaremos los diferentes casos por separado, aunque en principio debería ser una decisión[322] de los prestadores que expiden certificados tener un tipo diferente para órganos y otro para el resto de empleados públicos y personal, o tener un tipo único que cubra, con una semántica más compleja, todos los casos anteriores.

En ambos casos, resulta aplicable en su integridad la LFE, de forma que se deberá plantear la conveniencia de emitirlos como certificados reconocidos y, en su caso, en dispositivo seguro de creación de firma, lo que es recomendable en todo caso.

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, detenta una 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 jamás tener 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.

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 CATCert, 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

[322] Esta decisión, sin embargo, se ha visto muy afectada por el RDLAE y el RDENI y su desarrollo en el ámbito de la AGE por la política de certificación CertiCA.

Vascas.

6.2.1.1 El denominado certificado de órgano o cargo

El certificado de órgano no aparece mencionado de forma expresa en la LAE, aunque cabe considerarlo cubierto por el artículo 19 LAE, que en su apartado 1 determina que "sin perjuicio de lo previsto en los artículos 17 y 18, la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio, de acuerdo con lo dispuesto en los siguientes apartados".

Concreta el apartado 2 que "cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios".

Dentro de las posibilidades cubiertas por el artículo 19 cabe incluir a los empleados públicos, pero también a las personas que ocupan los órganos (unipersonales o colegiados), especialmente teniendo en cuenta la definición legal de empleado público que contiene la Ley 7/2007, de 12 de abril, por la que se aprueba el Estatuto Básico del Empleado Público, que deja a los órganos directivos y políticos fuera de dicha consideración.

En sentido similar, el artículo 21.1 de la LUTICAJ – en claro paralelismo con la LAE – establece que “sin perjuicio de lo previsto en los artículos 9 y 10 sobre la sede judicial electrónica, la identificación y autenticación del ejercicio de la competencia de la oficina judicial actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio, de acuerdo con lo dispuesto en los siguientes apartados”, para concretar a continuación las reglas de competencia para el otorgamiento de los citados sistemas:

“2. Las Administraciones, en el ámbito de sus competencias, proveerán a secretarios judiciales, fiscales, forenses y demás personal al servicio de la Administración de Justicia, de sistemas de firma electrónica, los cuales podrán identificar de forma

conjunta al titular del puesto de trabajo y el cargo e identificar también a la oficina u órgano judicial en la que presta sus servicios.

El Ministerio de Justicia facilitará a las Administraciones competentes datos actualizados de los fiscales y secretarios judiciales a fin de dotarles de firma electrónica.

3. Los sistemas de firma electrónica de jueces y magistrados serán los que provea el Consejo General del Poder Judicial. Este podrá establecer, a través de convenios, que el proveedor sea la Administración competente.

4. Las Administraciones, en el ámbito de sus competencias, dotarán de sistemas de firma electrónica a los representantes procesales del Estado y demás entes públicos, a los que se refiere el artículo 551 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial."

En cualquier caso, la posibilidad de emitir certificados a los órganos ya tenía apoyo legal directo en la propia LFE, como hemos tenido oportunidad de analizar *supra*[323].

6.2.1.2 Los certificados para empleados públicos

Una segunda clase de certificados de personal al servicio de las Administraciones Públicas serían los certificados emitidos a los empleados públicos, tal y como los mismos se definen en la legislación vigente.

En este caso, los certificados ofrecen la posibilidad de incluir también una gran variedad de informaciones útiles sobre los firmantes, permitiendo la integración de los sistemas de firma electrónica con los Registros de Personal legalmente exigibles, tanto para la expedición del certificado como para la posterior gestión de su ciclo de vida, o para comprobaciones de informaciones adicionales[324].

---

[323] Cfr. la sección 6.1.1.1 de este trabajo.

[324] URIOS APARISI (2012: pp. 912 y 913) se decanta por ambas posibilidades en su evaluación del sistema de firma electrónica que requieren los letrados autonómicos para la actuación empleando medios

La óptica de actuación interna de los empleados públicos, normalmente adscritos a unidades de tramitación dentro de la oficina administrativa, con vistas a la preparación de la resolución administrativa, ofrece un conjunto de casos más reducido y, en general, con menores consideraciones de riesgo que en los restantes tipos de certificados.

6.2.1.3 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 personal al servicio de la Administración.

Esta previsión es a nuestro juicio 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[325], 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.

---

electrónicos en el ámbito del procedimiento judicial, indicando que "lo más adecuado sería la utilización de un certificado de atributos [*rectius*, un certificado con atributos], si bien tampoco podría descartarse la utilización de un certificado que acreditara simplemente la identidad de la personas, y con una posterior consulta a un sistema de gestión de identidades, se certificara igualmente la habilitación para actuar en juicio".

[325] Caso que quiera utilizarlo, porque compartimos la opinión de URIOS APARISI (2012: pp. 915-915) sobre la dificultad de imponer la obligación de uso de los certificados del DNI-e en el ejercicio de funciones

- Aunque disponer del DNI-e como soporte físico es obligatorio, no se puede obligar a su titular 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[326].

- 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[327], por ejemplo).

VALERO TORRIJOS considera acertadamente, además, que "en cumplimiento del principio de calidad de los datos consagrado en el artículo 4 LOPD, se deberán adoptar las medidas que aseguren la opacidad de los datos personales necesarios para realizar los tratamientos informáticos que requieran las aplicaciones utilizadas, en especial el número de identidad fiscal", si bien este problema se puede plantear también en otros certificados electrónicos reconocidos, como los expedidos específicamente al personal de la Administración.

Quizá por todos estos límites, incluso la propia Policía Nacional, que emite el DNI-e, se ha dotado 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

---

públicas, incluso mediante una norma reglamentaria.

[326] En sentido similar, LINARES GIL, 2010: p. 436, que, además, considera que tampoco los empleados públicos tendrían un derecho al empleo del DNI electrónico en su actuación, con base en el artículo 21 del RDLAE.

[327] Así lo dispone la legislación vigente y lo recuerda la sección 4.1.1 de la Declaración de Prácticas de Certificación de la Policía Nacional.

público.

6.2.2 El 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.

En nuestra opinión, resulta criticable la defectuosa inclusión del sello dentro de los sistemas de firma electrónica, ya en esta ocasión por simple y directa contradicción entre sello y firma, que evidentemente son conceptos incompatibles[328].

Y es que resulta necesario considerar los problemas de la aplicación de la legislación

[328] En este sentido, el borrador de Reglamento europeo sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior, de 4 de junio de 2012, distingue adecuadamente entre la firma electrónica, en el caso de la persona física, y el sello electrónico, en el caso de la persona jurídica. Cfr. COM (2012) 238/2, accesible en http://ec.europa.eu/information_society/policy/esignature/docs/regulation/com_2012_2038_en.pdf (última visita: 25/06/2012).

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.

Como ejemplos particulares de problemas[329] a resolver en esta aplicación de la LFE 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, ex 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

[329] LINARES GIL (2010: pp. 459 y ss.) aprecia con acierto la dificultad de aplicar a estos certificados la regulación aplicable a los certificados electrónicos reconocidos que se contiene en la LFE. A su juicio, no parece que haya sido ésta la voluntad del legislador, de forma que debería entenderse aplicable únicamente el régimen general de la Ley. Asimismo, el autor nota la dificultad de determinar el procedimiento aplicable a la expedición de estos certificados y, en concreto, del cambio de los titulares del órgano que recibe un sello, cuando su identidad se incluya en el mismo, críticas con las que estamos completamente de acuerdo.

Administración de Justicia[330], establecen la necesidad de proceder a la creación de los sellos electrónicos mediante resolución[331], que se publicará en la sede electrónica correspondiente y en la que deberá constar:

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[332],

---

[330] Nótese que en la LUTICAJ se eleva a norma con rango de ley formal la previsión puramente reglamentaria contenida en el RDLAE, aplicable exclusivamente en la Administración General del Estado.

[331] En el ámbito de la Administración General del Estado, el artículo 19.1 del RDLAE atribuye la competencia a la Subsecretaría del Ministerio o titular del organismo público competente, mientras que la LUTICAJ se refiere a la autoridad competente, que deberá ser determinada conforme a ulteriores reglas de atribución.

[332] En todo caso, y como veremos posteriormente, a través de la política marco de firma electrónica y de certificados de la Administración General del Estado y, en concreto, del proyecto CertiCA, se han normalizado los perfiles de certificados de sello electrónico, norma que afecta a los certificados de sello expedidos a la Administración General del Estado, pero también a los sellos admitidos en las relaciones con dicha Administración, de forma que en la práctica, todos los sellos electrónicos siguen la misma

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, apuntado anteriormente, de establecimiento de límites en el empleo del sello.

En nuestra opinión, resulta 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[333].

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 "sello electrónico".

b) Nombre del suscriptor.

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

Resulta interesante ver que en estos contenidos mínimos sólo se considera la identidad del suscriptor, pero no de la persona titular del órgano, posibilidad que prevé la legislación. En nuestra opinión, 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[334], o una exposición innecesaria de los datos personales de dicha persona al

---

sintaxis y contenidos mínimos.

[333] De hecho, esta segunda opción puede plantear dudas jurídicas pero también de seguridad, especialmente en caso de robo de la clave privada de firma del sello, que permitiría producir cualquier documento administrativo aparentemente válido.

[334] Dado que en este caso, ya no sería correcta esta información y, en aplicación de la LFE, se deberá proceder a la retirada y sustitución del certificado en cuestión, lo cual genera esfuerzos y costes

público[335].

Finalmente, los artículos 19.3 del RDLAE y 20.3 de la LUTICAJ remiten al correspondiente Esquema Nacional "el modo de emitir los certificados electrónicos de sello electrónico", previsión que llama la atención poderosamente por la – en el mejor caso – escasa conexión entre ambas materias. De hecho, aunque el RDLAE se realizó esta previsión, el Esquema Nacional de Seguridad estaba pendiente de aprobación, y en el texto finalmente aprobado no se ha incluido ninguna previsión concreta al respecto[336].

En cambio, el artículo 33.2 del RDENS lacónicamente indica que "la política de firma electrónica y de certificados concretará los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas, sin perjuicio de lo previsto en el Anexo II, que deberá adaptarse a cada circunstancia".

Como se puede ver, se realiza un renvío completo, en cuestión del ciclo de vida de la firma electrónica y de sus elementos accesorios, como los certificados y los sellos de fecha y hora, a la política de firma electrónica y de certificados, que expondremos a continuación.

innecesarios.

[335] En este punto, se debería evaluar si este tratamiento de datos personales es verdaderamente compatible con los principios legales aplicables, en particular porque se puede considerar que se trata de una divulgación innecesaria de los datos de identidad de la persona afectada que, de hecho, no actúa, por tratarse de un automatismo.

[336] Por lo que aún llama más la atención que también la LUTICAJ considere una previsión similar, si bien en este caso se realiza al Esquema Judicial de Interoperabilidad y Seguridad.

6.3 LA POLÍTICA DE FIRMA RESTRINGE LOS CERTIFICADOS APLICABLES

En primer lugar, el apartado 1 del citado epígrafe IV.1 establece, con carácter general, que "las políticas de firma, marco o particulares, podrán fijar limitaciones y restricciones específicas para los certificados electrónicos que admiten en cada uno de los servicios que corresponda, siempre en consideración de la normativa aplicable en cada caso".

Se trata de una cláusula excesivamente abierta, a nuestro juicio, que sólo puede entenderse aceptable en términos descriptivos, pero en estricta sujeción a la normativa que anteriormente hemos presentado sobre la admisión de certificados.

En efecto, sencillamente no se podría considerar que este apartado contenga una habilitación de selección absolutamente discrecional de certificados por parte de la Administración, porque como sabemos los ciudadanos gozan de un derecho de admisión de los sistemas de firma electrónica basados en certificados electrónicos reconocidos que cumplen el artículo 21.1 de la LAE y 22.1 de la LUTICAJ.

Quizá para evitar este problema, el apartado 2 del epígrafe IV.1 de la Norma Técnica de Interoperabilidad de la política de firma electrónica y de certificados de la Administración indica que "los certificados válidos para ejecutar la firma electrónica de contenido serán los siguientes:

a) Cualquier certificado electrónico reconocido según la Ley 59/2003, de 19 de diciembre, y la Directiva 1999/93/CE, de 13 de diciembre de 1999.

b) Nuevas tipologías de certificados definidos en la Ley 11/2007, de 22 de junio".

Se trata, de hecho, de una orientación aparentemente muy liberal, que sin embargo resulta criticable, porque de entrada limita la firma de contenidos a los mecanismos basados en certificados electrónicos reconocidos, en infracción de la potestad de la

Administración de admitir otros sistemas de firma electrónica[337].

En nuestra opinión, se debe entender esta regla en un sentido "de mínimos", de forma que al menos se deban admitir estos certificados para la firma de contenidos, pudiendo cada Administración admitir otros.

Por otra parte, también resulta defectuosa la referencia a "los nuevos tipos de certificados definidos en la Ley 11/2007, de 22 de junio", dada la ambigüedad de la fórmula empleada, en especial en relación con los certificados de sede electrónica, que al menos en el ámbito de la Administración General del Estado no pueden emplearse para la firma electrónica de contenidos, según dispone el artículo 18.2 del RDLAE.

6.3.1 La discriminación de los certificados de atributos

La Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración realiza una decidida apuesta por el empleo de certificados de clave pública, en detrimento de otros tipos de certificados como los de atributos, que hemos presentado *supra*[338].

El uso de certificados de atributos[339] en la firma electrónica ha sido normalizado técnicamente en los estándares más habituales y, desde luego, las condiciones y reglas técnicas correspondientes se encuentran perfectamente especificadas en XAdES, CAdES y PAdES.

Sin embargo, resulta necesario poner de manifiesto que la Norma Técnica de Interoperabilidad de política de firma electrónica no permite el empleo de certificados de atributos, restricción que a nuestro juicio resulta poco justificada.

---

[337] Cfr. artículo 21.2 de la LAE y 22.1 de la LUTICAJ.

[338] Véase la sección 6.1.1 de este trabajo.

[339] Nos referimos a los certificados de atributos, que sólo contienen estas informaciones, pero no clave pública, y no a los certificados de clave pública con atributos adicionales, que sí resultan admisibles, pero no sin problemas.

Se trata de una prohibición implícita, que se deduce de una lectura más bien profunda de la Norma Técnica de Interoperabilidad:

- Por una parte, de la limitación de uso de certificados reconocidos de acuerdo con la LFE para la firma de contenidos que se contiene en la regla 2 del epígrafe IV.1, dado que obviamente los certificados de atributos no cumplen los requisitos legalmente establecidos para dichos tipos de certificados[340].

- Por otra, de lo establecido por la regla 4 del epígrafe III.6, en relación con la regla 5 del mismo epígrafe III.6 y el anexo I, ya que la única forma de indicar un rol de actuación es alegarlo; esto es, no se permite la inclusión de certificados de atributos dentro de la firma electrónica.

Entrando en el detalle concreto, el apartado III.6.4 indica que "como datos opcionales, la firma podrá incluir: […] b) Rol de la persona firmante en la firma electrónica". Los estándares técnicos de referencia anteriormente indicados ofrecen dos opciones para incluir esta información:

- Rol alegado (*claimed role*), que consiste en añadir un atributo dentro de la firma electrónica que contiene una cadena de texto indicado dicho rol. Se denominado "alegado" porque realmente este texto es aportado por el firmante, y no se encuentra previamente verificado por nadie. La alegación se protege mediante la extensión de la firma electrónica sobre dicho atributo, de forma que el texto no puede ser alterado una vez se ha generado la firma.

  Por ejemplo, se podría incluir la alegación "Administrador único" dentro de la firma electrónica, de forma que la Administración podría hacer uso de esta información, en su caso exigiendo la correspondiente documentación de contraste.

- Rol certificado (*certified role*), que consiste en incluir dentro de la firma

[340] En concreto, y como hemos expuesto en la sección 6.1.1 de este trabajo, estos certificados no tienen una clave pública asociada.

electrónica precisamente un certificado de atributos, emitido por el correspondiente prestador, con las garantías oportunas. Dicho certificado se incluye en una estructura de datos especial que permite su lectura y verificación fiables, como en el caso de los restantes certificados.

Aplicado al mismo ejemplo, podríamos imaginar que el Registro Mercantil emita certificados de atributos, de duración temporal limitada a un día, certificando la condición de administrador único del titular. En este caso, una vez verificado el certificado, la Administración podría confiar directamente en este dato, con la consiguiente simplificación del procedimiento, y un ahorro de costes asociado[341].

Como hemos adelantado, el epígrafe III.6.5 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración especifica que "la información indicada en los epígrafes 3 y 4 del presente subapartado se recogerá en cada formato de firma según las etiquetas del anexo", anexo que especifica que el rol de la persona, que es opcional, se deberá incluir empleando el elemento SignerRole – ClaimedRoles, en XAdES, o el atributo Signer-attributes, en CAdES y PAdES.

Si comparamos ambos tipos en los estándares aplicables, rápidamente veremos que en el caso de XAdES se permite únicamente el rol alegado, mientras que en los otros dos casos parece que no se establece esta restricción, y por tanto resultaría posible emplear roles alegados o certificados de forma indistinta.

En caso afirmativo, nos encontraríamos ante un tratamiento diferente de una misma situación únicamente apoyada en la sintaxis del formato de la firma, lo cual resultaría de todo punto inaceptable, por lo que parece que debemos quedarnos con la interpretación que parte de que en ningún formato de firma electrónica avanzada se pueden emplear certificados de atributos.

[341] Es de imaginar que el Registro Mercantil cobraría por la expedición de este certificado de atributos, pero aun así se produciría un ahorro tanto para el ciudadano, que se ahorraría el coste de hacer llegar el documento a la Administración, y para la Administración, que no precisaría del acto administrativo de verificación de dicha documentación.

Resulta a todas luces evidente la ventaja que suponen los certificados de atributos. Sin negar los posibles retos en su uso, en nuestra opinión la opción de restringir su empleo es criticable, no se encuentra basada en la Decisión de la Comisión 2011/130/UE, de 25 de febrero[342], y resulta conveniente ampliar en un futuro cercano la Norma Técnica de Interoperabilidad para regular su empleo.

6.3.2 Sobre la interoperabilidad – ¿o uniformización? – de los certificados para la firma de la Administración

El régimen del certificado corporativo de empleado público[343] y de sello electrónico para la actuación administrativa automatizada, ha sido desarrollado muy detalladamente en el ámbito de la Administración General del Estado en el marco del proyecto CertiCA del Consejo Superior de Administración Electrónica, en cumplimiento de lo establecido en los artículos 24.1 del RDLAE y 18.4 del RDENI.

Recuérdese que éste último determina que "los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones sin ningún tipo de restricción técnica, semántica u organizativa. Dichos certificados serán los definidos en la Ley 11/2007, de 22 de junio, la Ley 59/2003, de 19 de diciembre, de firma electrónica y sus desarrollos normativos", motivo por el cual se ha desarrollado una política de certificación, y los correspondientes perfiles de certificados (CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, 2010a.).

---

[342] De hecho, incluso aunque la citada Decisión restringiese el empleo de estos certificados, resultaría sólo aplicable a la generación de documentos firmados por las Autoridades Competentes en el marco de la Directiva de Servicios, mientras que en la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados la restricción se extiende incluso a los documentos producidos por los ciudadanos.

[343] Así como del certificado de órgano, que se consideran, en general, como una subclase de los certificados de empleado público, posición con la que no nos encontramos necesariamente de acuerdo.

Este último documento se describe a si mismo como "documento de referencia para los certificados derivados de la LAECSP (Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos), de acuerdo con las diversas configuraciones acordadas, atendiendo a los diferentes niveles de aseguramiento", y define, en lo que ahora nos interesa[344], los siguientes contenidos:

- Caracterización de los perfiles de certificados (sección 2), donde se describen los campos que componen los diferentes perfiles, incluyendo campos obligatorios[345] y campos opcionales, y recomendaciones sobre los niveles de aseguramiento (medio y alto).

  Respecto a estos niveles de aseguramiento, se establece que "se determina un esquema de garantía para las aplicaciones y servicios electrónicos que deseen establecer los medios de identificación y autenticación electrónicos. Se establecerá el nivel de riesgo asociados al caso de uso concreto, y en consecuencia, se determinarán los mecanismos de identificación y autenticación admitidos", y a continuación se "se definen dos niveles de aseguramiento:

  - Nivel medio:

    - Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para la mayoría de aplicaciones.

    - El riesgo previsto por este nivel (siguiendo la recomendación de la OCDE):

      - Infracción de seguridad (ej: el robo de identidad)

      - Puede producir pérdidas económicas moderadas

[344] No presentamos los contenidos del certificado de sede electrónica, ya que el mismo no se emplea para la firma de contenidos.

[345] En línea con los contenidos del RDLAE y de la LUTICAJ a que nos hemos referido en la sección 6.2 de este trabajo.

- Pérdida de información sensible o crítica.
- Refutación de una transacción con impacto económico significativo.

- Asimismo, el riesgo previsto por este nivel corresponde al nivel 3 de garantía previsto en la Política Básica de Autenticación de IDABC.
- Los mecanismos de seguridad aceptables incluyen los certificados X.509 en software. En los casos de certificados emitidos a personas, se corresponde con el de un 'certificado reconocido', como se define en la Ley 59/2003, de firma electrónica, para firma electrónica avanzada, sin dispositivo seguro de creación de firma.

- Nivel alto:
  - Este nivel corresponde a una configuración de mecanismos de seguridad apropiada para las aplicaciones que precisan medidas adicionales, en atención al análisis de riesgo realizado.
  - El riesgo previsto por este nivel (siguiendo la recomendación de la OCDE):
    - Infracción de seguridad
    - Puede producir pérdidas económicas importantes
    - Pérdida de información altamente sensible o crítica.
    - Refutación de una transacción con impacto económico muy significativo.
  - Asimismo, el riesgo previsto por este nivel corresponde al nivel 4 de garantía previsto en la Política Básica de Autenticación de IDABC.

- Los mecanismos de seguridad aceptables incluyen los certificados X.509 en hardware. En los casos de certificados emitidos a personas, se corresponde con el de 'firma electrónica reconocida', como se define en la Ley 59/2003, de firma electrónica."

- Normas sobre uso de identificadores de objeto (sección 3), básicamente a efectos de los campos nuevos que se definen en la política.

- Definición de la identidad administrativa (sección 4), mediante la normalización de los campos "SubjectName" y "SubjectAlternativeName" de los certificados, incluyendo una propuesta de nombre diferenciado "para la identificación inequívoca de personas físicas y suscriptores de certificados, para facilitar su procesamiento eficiente por aplicaciones automáticas, aun resultando redundante con la información ya contenida en otros campos.

  Esta identidad, que denominamos 'identidad administrativa', la puede construir el prestador, de forma que se disponga de toda la información de forma homogénea dentro del certificado, especialmente debido a que algunos componentes de los nombres tienen semántica diferente, en función del tipo de certificado".

- Guía para la cumplimentación de los campos de los certificados (sección 5), con "la finalidad […] de emplear los mismos nombres para todos los certificados de forma que exista un marco común. De este modo se asignará exactamente el mismo nombre a sellos, sedes, organizaciones, puestos y unidades, etc. para toda la Administración Pública Estatal".

- Requisitos en relación con el uso de algoritmos (sección 6). En concreto, "se establece un escenario de seguridad básico denominado 'entorno de seguridad genérico de la AGE', que determinará el criterio de robustez y viabilidad aplicable para cada perfil de certificado. Los dos niveles de aseguramiento recogidos en apartado 2 del presente documento se considerarán dentro de dicho escenario.

Adicionalmente y al amparo del artículo 4.4 de la LFE (uso de la firma electrónica en entornos sensibles para la seguridad pública, la defensa nacional, el manejo de información clasificada) podría establecerse un entorno de alta seguridad para los prestadores o Administraciones que así lo requieran. Dicho entorno estaría fuera del alcance de este documento y debería seguir las recomendaciones de la guía CCN-STIC 405, que alinea los algoritmos y longitudes de clave frente a las amenazas de las que hay que proteger hoy día la información clasificada nacional o internacional (OTAN, UE, etc.)."

- Perfil del certificado de autoridad de certificación subordinada[346] (sección 7), que describe los contenidos de un certificado empleado por un prestador de servicios de certificación para la expedición de certificados a los usuarios finales.

- Perfil del certificado de sello electrónico (sección 9), que describe los contenidos de este tipo de certificado, siempre con la condición de certificado reconocido[347], diferenciando los campos comunes de los específicos para el nivel de aseguramiento alto y el medio.

  Esencialmente, el certificado de sello electrónico de nivel alto se diferencia del de nivel medio porque cumple las condiciones para la firma electrónica reconocida previstas en la LFE; esto es, exige el empleo de algoritmos robustos (SHA-1/SHA-2 con RSA de clave 2048) y empleo de dispositivo seguro de creación de firma electrónica (con indicación de esta condición dentro del propio certificado).

[346] Nótese que el certificado raíz de la jerarquía no se regula sino levemente, y de forma indirecta, en nuestra opinión, acertadamente.

[347] Resulta notable esta elección, que no viene desde luego impuesta por la legislación. En efecto, el artículo 18.1.a) de la LAE se refiere al "sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica", de modo que se podría haber optado, perfectamente, por el empleo de un certificado electrónico sin la consideración de reconocido. Pero claro, como hemos visto anteriormente, sección 6.1.3, sólo el certificado reconocido ofrece garantías legales mínimas de identificación, por lo que seguramente resulta más fácil obtener un sello de actuación automatizada fiable si se alinea con el certificado reconocido que especificando los requisitos a partir de la casi nula regulación del certificado ordinario en la LFE.

Por el contrario, en el nivel medio resulta suficiente con el empleo del algoritmo SHA-1/SHA-2 con RSA de clave 1024) y se puede emplear un certificado en cualquier soporte, lo cual apuntaría a la consideración de este sistema como firma electrónica avanzada, si bien basada en certificado reconocido.

- Perfil del certificado de empleado público (sección 10), que describe los contenidos de este tipo de certificado, diferenciando los campos comunes de los específicos para el nivel de aseguramiento alto y el medio.

  De nuevo, la diferencia esencial entre los certificados de empleado público de nivel alto respecto a los de nivel medio es la alineación del nivel alto – en este caso con una interpretación muy estricta – con la firma electrónica reconocida, incluyendo no sólo el empleo de algoritmos robustos (SHA-1/SHA-2 con RSA de clave 2048) y de dispositivo seguro de creación de firma electrónica (con indicación de esta condición dentro del propio certificado), sino además la total segregación de claves[348], de forma que el empleado público recibe una tarjeta criptográfica con tres certificados, para identificación, firma y cifrado[349].

  Por el contrario, en el nivel medio resulta suficiente con el empleo del algoritmo SHA-1/SHA-2 con RSA de clave 1024) y se puede emplear un certificado en cualquier soporte, y con cualquier combinación de uso de claves, lo cual apuntaría a la consideración de este sistema como firma electrónica avanzada, si bien basada en certificado reconocido[350].

Como se puede ver, se trata de una muy completa definición de la regulación de los

[348] La especificación técnica ETSI TS 102280: pp. 10-11, así lo recomienda, para garantizar al máximo que el empleo de la clave de compromiso con el contenido (irrefutabilidad) no se emplea en operaciones de simple identificación.

[349] Constituyen ejemplos de sistema de firma electrónica de empleado, nivel alto, el carné profesional del Cuerpo Nacional de Policía (Orden INT/761/2007, de 20 de marzo) o del personal del Ministerio de Defensa (Orden 3/2008, de 8 de enero).

[350] En este punto el documento se separar de la prohibición de ETSI TS 102280: p. 10, de no permitir, en ningún caso, el empleo de un certificado reconocido para operaciones de cifrado, restricción del documento del ETSI que no podemos entender razonable ni acertada.

certificados de la LAE, previsiblemente extensible a la LUTICAJ, y en virtud de la cual, con la justificación de la interoperabilidad, lo que realmente sucede es que se normalizan todos los perfiles de certificados, con independencia de qué prestador de servicios de certificación los expida.

Dada la consideración de la Administración General del Estado como principal cliente consumidor de certificados electrónicos en España, los prestadores de servicios de certificación se han visto abocados a la adopción de estos perfiles[351], con el consiguiente efecto práctico de la uniformización de los certificados.

De hecho, no parece necesariamente negativa, en sí, la normalización de los certificados, y efectivamente favorece la admisión y la interoperabilidad en su uso, pero a nuestro juicio esta cuestión se ha tratado de forma insatisfactoria por diversas cuestiones de procedimiento:

- En primer lugar, el documento de perfiles de certificados al que nos referimos ha sido preparado y es gestionado por el Consejo Superior de Administración Electrónica, que es un órgano de la Administración General del Estado.

- En segundo lugar, se trata de un documento que indudablemente establece condiciones generales adicionales al uso de la firma electrónica en el ámbito de la Administración General del Estado, y con efectos materialmente idénticos para las restantes Administraciones, pero que no se ha tramitado en los términos que al efecto hemos visto que establece[352] la normativa aplicable.

- En tercer lugar, ni el RDENI ni el RDENS, ni por supuesto, la Norma Técnica de Interoperabilidad han establecido ninguna regla al respecto, y ello a pesar de la

[351] En el caso de los prestadores públicos de servicios de certificación, hay que decir que estos perfiles de certificados fueron presentados y, en principio, consensuados, en el marco de las reuniones de los grupos de trabajo de interoperabilidad liderados por el Ministerio responsable. Por lo que respecta a los prestadores privados, no parece que esta aproximación les haya perjudicado, puesto que una de sus principales preocupaciones ha sido evitar el riesgo de la aparición de condiciones técnicas de contenido que impidan que el certificado que expiden no sea utilizable en cualquier Administración, riesgo que de hecho nace de una interpretación patológica de la excepción del sector público.

[352] Cfr. sección 1.4.1 de este trabajo. De hecho, ni siquiera ha sido publicado en el BOE.

previsión expresa en este sentido que se contiene en el RDLAE.

Se podría haber obtenido un efecto similar en el contexto de un sistema voluntario de certificación de la actividad de los prestadores de servicios de certificación que expidan certificados para su uso en la Administración electrónica, con un modelo de gobernanza adecuado, por ejemplo alineado con lo establecido en el artículo 42 de la LAE[353], en cuyo contexto se podría realmente desarrollar el tratamiento de los certificados en la actual Norma Técnica de Interperabilidad, o en una Norma Técnica específica.

6.3.3 La dificultad de determinar el nivel de aseguramiento de los certificados a emplear

Merece un análisis particular el tratamiento de los niveles de aseguramiento ofrecidos por los certificados, tanto de los de la Administración, como de los certificados de los ciudadanos.

Ya hemos visto anteriormente que, en general, todo certificado reconocido es admisible[354], y sin tener nada que objetar, desde luego, al establecimiento de dos niveles diferentes de aseguramiento para los certificados, que de hecho presentan una fuerte equivalencia con los niveles de firma electrónica avanzada y reconocida[355], lo cierto es que para la determinación de en qué casos resulta aplicable uno u otro nivel – que no se encuentran regulados, ni siquiera mencionados, en la reglamentación (ni en el RDLAE, ni en el RDENI ni, finalmente, en el RDENS) – resulta necesario establecer algún criterio.

Esto permitirá proceder a la selección del certificado correspondiente, en el contexto de la concreta política de firma electrónica, como hemos visto prevé la regla 1ª del epígrafe IV.1 de la Norma Técnica de Interoperabilidad de Política de firma electrónica

[353] Y su correlativo en la LUTICAJ.

[354] Cfr. sección 2.1.3 de este trabajo.

[355] Cfr. sección 1.3 de este trabajo.

y de certificados de la Administración.

La cuestión del nivel de aseguramiento del certificado se puede resolver, ciertamente tanto en el caso de los certificados de ciudadanos como en el los certificados de la Administración, mediante la realización de un análisis de riesgos, pero en nuestra opinión cabe aplicar, en primer lugar, las reglas de certificación que contempla el RDENS, contenidas en el epígrafe 5.7.4:

- En el nivel bajo se empleará cualquier medio de firma electrónica de los previstos en la legislación vigente, por lo que, en principio, no se establecería restricción ninguna en cuanto a los algoritmos a emplear.

- En el nivel medio, se establece que se emplearán, preferentemente, certificados reconocidos y dispositivos seguros de firma.

- En el nivel alto, se indica que se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en el nivel medio, además del empleo obligatorio de certificados reconocidos y dispositivos seguros de creación de firma.

La lectura de esta norma resulta muy llamativa, por lo liberal del enfoque que plantea, al menos en términos de seguridad mínima exigible a los certificados electrónicos y, en su caso, dispositivos asociados.

En efecto, el nivel bajo de seguridad en las dimensiones de autenticidad e integridad permite cualquier tipo de certificado, y el nivel medio sólo recomienda el empleo de certificados reconocidos y de dispositivos seguros, por lo que se trata, como puede comprenderse fácilmente, de una norma menos exigente[356] incluso que la LAE y, por supuesto, la LUTICAJ que, como hemos podido analizar con detalle, sólo garantizan el derecho de admisión a los certificados reconocidos.

En este sentido, todos los certificados cubiertos por el derecho de admisión serán válidos para su uso en sistemas de información que ofrezcan soporte a procedimientos

[356] No es menos exigente, en cambio, en materia de algoritmos criptográficos que, como hemos visto, en nivel medio deben encontrarse acreditados por el CCN-CERT. Cfr. la sección 5.2 de este trabajo.

electrónicos categorizados con este nivel medio, y por supuesto, también lo serán los certificados que la política de certificación CertiCA cualifica como de nivel medio, por ser reconocidos. Eso sí, los algoritmos a emplear deben ser aquellos que haya acreditado el órgano competente, que como sabemos es el Centro Criptológico Nacional.

Respecto a los sistemas de información de nivel alto, en este caso se exige el certificado reconocido y el dispositivo seguro de creación de firma, constituyendo una restricción – entendemos que plenamente justificada – a la admisión del certificado en que se basa el sistema de firma electrónica.

En consecuencia, cuando la Administración actúe como firmante, deberá dotarse de certificados de empleado público o de sello electrónico cualificados como de nivel alto en la política de certificación CertiCA que hemos presentado anteriormente.

6.4 CÓMO REGULAR DE NUEVO A LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN, CON LA EXCUSA DE LA INTEROPERABILIDAD

La regla 3ª del epígrafe IV.1 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración establece la regla de que "los requisitos a cumplir por los prestadores de servicios de certificación en relación con la interoperabilidad organizativa, semántica y técnica serán los establecidos en el artículo 21 de la Ley 11/2007, de 22 de junio, en el artículo 19 del Real Decreto 4/2010, de 8 de enero, y en el resto de normativa aplicable en cada caso".

Al artículo 21.1 de la LAE hemos tenido ya ocasión de referirnos en el estudio del que hemos denominado "derecho de admisión"[357], siendo ahora únicamente necesario recordar la triple condición de tratarse de un certificado reconocido, que el prestador de servicios de certificación ponga a disposición de las Administraciones Públicas la

[357] En relación con la admisión de certificados, véase la sección 2.1.2 de este trabajo.

información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas.

6.4.1 Las "obligaciones de interoperabilidad" de los prestadores de servicios de certificación

Sin embargo, el artículo 19 del RDENI, bajo el aparentemente inocuo título de "aspectos de interoperabilidad relativos a los prestadores de servicios de certificación", añade un importante paquete de obligaciones adicionales, que entendemos deben ser consideradas como condiciones adicionales generales al uso de la firma electrónica y, por tanto, cumplir los requisitos del artículo 4 de la LFE.

El apartado 1 del artículo 19 del RDENI indica que "de acuerdo con lo previsto en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, sobre obligaciones de los prestadores de servicios de certificación, en relación con la interoperabilidad, dichos prestadores cumplirán con lo indicado en los apartados siguientes", previsión que nos parece criticable atendido el diverso alcance subjetivo de ambas normas; mientras que el RDLAE sólo resulta aplicable a la Administración General del Estado, el RDENI afecta a todas las Administraciones Públicas.

No parece la mejor técnica reglamentaria mezclar ambas normas como si de vasos comunicantes se tratase, dado el diverso alcance subjetivo de ambas normas. Cabe, en todo caso, deducir que la referencia al RDLAE que contiene el RDENI proviene de la sujeción de los prestadores al cumplimiento de las condiciones adicionales que se establezcan (cfr. artículo 23.1 del RDLAE). Pero claro, eso supone una interferencia absolutamente injustificada por parte del nivel de administración estatal hacia las restantes Administraciones, que no tiene base legal y es, en nuestra opinión, manifiestamente ilegal.

Además, existen serias dudas acerca del cumplimiento por estas condiciones adicionales, de los requisitos legales de objetividad, proporcionalidad, transparencia y no discriminación, y no obstaculización de la prestación de servicios de certificación al

ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.

Como veremos, algunas de estas condiciones infringen el Derecho europeo, por lo que deben considerarse ilegales y de imposible aplicación a los prestadores europeos de servicios de certificación: sólo haciendo una interpretación tan amplia de las citadas condiciones que conduzca a su inaplicación práctica se pueden salvar las mismas, por lo que, en nuestra opinión, hubiese sido mejor no establecerlas. Excepción hecha, claro, de contribuir a una inflación reglamentaria de baja eficacia[358].

El apartado 2 del propio artículo 19 del RDLAE establece que "en relación con la interoperabilidad organizativa[359], los prestadores de los servicios de certificación dispondrán de lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) Establecimiento de los usos[360] de los certificados expedidos de acuerdo con un perfil dado y sus posibles límites de uso[361].

b) Prácticas al generar los certificados que permitan posteriormente la aplicación de unos mecanismos de descubrimiento y extracción inequívoca de los datos de identidad[362] del certificado.

c) Definición de la información de los certificados o relacionada con ellos que será

---

[358] Mejor hubiese sido, en nuestra opinión, la aprobación de un reglamento de la LFE aplicable con carácter general.

[359] Recuérdese que el RDENI define la interoperabilidad organizativa como "aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan".

[360] Esto se realiza, normalmente, mediante el empleo de un campo concreto dentro del certificado, denominado Key Usage, de uso más o menos normalizado. Cfr. ITU-T X.509v3, IETF RFC 5280, ETSI TS 102 280 o los perfiles comunes de certificados electrónicos de la Ley 11/2007 del proyecto CertiCA.

[361] Para los límites de uso se ha definido un campo específico del certificado X.509 que permite su inclusión, en particular en relación con el límite económico, que sin embargo plantea problemas de interoperabilidad semántica dada la diferente interpretación de la limitación, y de las consecuencias en caso de infracción (Cfr. ETSI TS 102 862).

[362] Aspecto ciertamente necesario para la correcta identificación del firmante, que elimine las ambigüedades potenciales, y que facilita a la Administración usuaria la programación de sus aplicaciones de firma electrónica. Se refiere especialmente al empleo de los campos Subject Name y Subject Alternative Name, donde se contiene la identidad del firmante, empleando diversas técnicas.

publicada por parte del prestador, debidamente catalogada[363].

d) Definición de los posibles estados en los que un certificado pueda encontrarse a lo largo de su ciclo de vida.

e) Los niveles de acuerdo de servicio definidos y caracterizados para los servicios de validación y de sellado de fecha y hora".

Las previsiones contenidas en estos apartados d) y e) resultan muy relevantes. En efecto, es necesario conocer el plazo comprometido por el prestador que expide el certificado cuando el mismo es suspendido o revocado en relación con la difusión pública de dichas incidencias, debido a que sólo transcurrido este plazo se podrá verificar de forma fiable la firma electrónica.

La LFE indica, en su artículo 10.1 que "el prestador de servicios de certificación hará constar inmediatamente, de manera clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia", pero no se concreta más, por lo que cual existe una cierta incertidumbre que debe encontrarse limitada a un plazo máximo razonable[364], a fin y efecto de garantizar una mínima seguridad jurídica a los receptores de documentos firmados[365].

El apartado 3 del artículo 19 del RDENI, por su parte, indica que "en relación con la interoperabilidad semántica[366], los prestadores de servicios de certificación aplicarán

[363] Previsión que apunta a la determinación, en particular, de la información de estado de certificados necesaria para su validación.

[364] La política de firma electrónica, como veremos, trata esta cuestión en forma de periodo de gracia para la validación y sellado de la firma electrónica.

[365] ETSI TS 101 456, que establece buenas prácticas en la expedición y gestión de certificados electrónicos reconocidos, se refiere a un plazo máximo de 24 horas, si bien la mayoría de prestadores intentan reducir este plazo indicando que los cambios de estado se publican cuando se producen, sin espera alguna.

[366] La interoperabilidad semántica se define en el RDENI como "aquella dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación".

lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) La definición de los perfiles de certificados[367] que describirán, mediante mínimos, el contenido obligatorio y opcional de los diferentes tipos de certificados que emiten, así como la información acerca de la sintaxis y semántica de dichos contenidos.

b) Establecimiento de los campos cuya unicidad de información[368] permitirá su uso en labores de identificación".

Finalmente, el apartado 4 del artículo 19 del RDENI establece que "en relación con la interoperabilidad técnica[369], los prestadores de los servicios de certificación aplicarán lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) Los estándares relativos a políticas y prácticas de certificación y generación de certificados electrónicos, estado de los certificados, dispositivos seguros de creación de firma, programas controladores, dispositivos criptográficos, interfaces de programación, tarjetas criptográficas, conservación de documentación relativa a los certificados y servicios, límites de los certificados, conforme a lo establecido en el artículo 11.

b) La incorporación, dentro de los certificados, de información relativa a las direcciones de Internet donde se ofrecen servicios de validación por parte de los prestadores.

c) Los mecanismos de publicación y de depósito de certificados y documentación asociada admitidos entre Administraciones públicas".

---

[367] Aunque los perfiles de certificados; esto es, las plantillas o modelos lógicos que se emplean para su expedición, se encuentran muy normalizados (cfr. ITU-T X.509v, IETF RFC 5280, ETSI TS 101 862, ETSI TS 102 280, entre otras especificaciones técnicas), existen muchas opciones y combinaciones posibles de campos, lo cual dificulta su interpretación automatizada y la comprensión de las condiciones de empleo por parte de los receptores de documentos firmados, por lo cual resulta apropiado establecer la obligación de documentarlos adecuadamente.

[368] En sentido similar al punto b) del apartado 2 del mismo artículo 19 del RDENI, resulta imprescindible evitar la homonimia de firmantes, por lo cual se exige poder identificar de forma unívoca al firmante.

[369] La interoperabilidad técnica se define en el RDENI como "aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga".

Todas estas condiciones adicionales parecen razonables, especialmente si entendemos que se tratan esencialmente de obligaciones informativas, que no afectan de forma desproporcionada a la libertad de los prestadores de servicios de certificación de operar en el mercado, pero sigue siendo necesario aconsejar una interpretación laxa de las mismas, que no discrimine a los prestadores de otros Estados miembro de la Unión Europea, so pena de infracción de la DFE y la LFE.

En particular, a nuestro juicio resultan incompatibles con el derecho europeo las condiciones adicionales previstas en el apartado 4 del artículo 19 del RDENI, por cuanto obligan al empleo de determinadas categoría de estándares y obligan a incluir dentro de los certificados campos que no son obligatorios para la expedición y funcionamiento de los certificados, aunque ciertamente lo facilite mucho.

Se trata, además, de previsiones que no encuentran apoyo legal en ninguna Decisión de la Comisión Europea, lo cual aún dificulta más su justificación en el contexto de operaciones transfronterizas.

6.4.2 El certificado reconocido de firma electrónica debe aparecer en la lista de servicios de confianza

Adicionalmente, la regla 4ª del epígrafe IV.1 de la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración indica que "la relación de prestadores de servicios de certificación que emiten certificados reconocidos se podrá consultar en la TSL (Lista de servicios de confianza) publicada en la sede electrónica del Ministerio de Industria, Turismo y Comercio".

Se trata de una regla que nos resulta sumamente criticable por diversos motivos. En primer lugar, porque el citado Ministerio es competente únicamente para la supervisión de los prestadores de servicios de certificación que expiden al público, como dispone el artículo 29.1 de la LFE, pero no para supervisar a los restantes prestadores de servicios de certificación.

Y es que el artículo 21.1 de la LAE, ni su correlativo artículo 22.1 de la LUTICAJ, no

establece como requisito para la admisión de los certificados que los mismos sean expedidos al público, por lo que resulta difícil entender la conexión entre supervisión y publicación de los certificados en la TSL.

En segundo lugar, porque de entenderse que la publicación del certificado en la TSL es condición previa para la admisión de certificados, estaríamos frente a una condición absolutamente discriminatoria y, por tanto, ilegal.

Además, se debería acudir, no a la TSL con los prestadores españoles, sino también a las correspondientes TSL de los restantes Estados miembros de la Unión Europea.

Dicho lo cual, bien es cierto que la TSL es un mecanismo avalado y promocionado por la propia Unión Europea, y un medio eficaz para difundir la información sobre los prestadores de servicios de certificación que expiden los diversos tipos de certificados electrónicos, por lo que seguramente a los prestadores de servicios de certificación ya les resulte conveniente aparecer en dicho instrumento.

7 CONCLUSIONES

En este estudio hemos analizado las políticas de firma electrónica y de certificados en la reglamentación de Administración electrónica, para lo cual hemos presentado también el régimen general de la firma electrónica, los principales tipos de certificados electrónicos aplicables y el régimen de utilización de la firma electrónica en el sector público, análisis del cual podemos extraer las siguientes conclusiones:

Primera.- Las políticas de firma electrónica y de certificados son, efectivamente, potentes herramientas para la interoperabilidad, que permiten facilitar los procesos de firma electrónica y garantizar el posterior intercambio y reconocimiento mutuo de los documentos firmados.

La aprobación de las políticas de firma electrónica y de certificados se realiza mediante un acto administrativo de decisión, atendida la naturaleza no reglamentaria de las citadas políticas, y requiere de su publicación, en lenguaje natural e informático, al menos en la sede electrónica del órgano emisor.

Segunda.- El efecto jurídico principal de la aplicación de una política de firma electrónica y de los certificados es la aceptación obligatoria de la firma electrónica sujeta a la misma, tras la comprobación de su validez y aplicabilidad al caso concreto, o, por el contrario, su denegación motivada, con las consecuencias jurídico-administrativas correspondientes.

En ambos casos, se trata de verdaderos actos administrativos de validación y constancia, de producción automatizada, que deberían ser objeto de un análisis detallado, en especial en atención al gravamen que supone para los ciudadanos la imposibilidad de presentar documentación a los registros electrónicos cuando no cumplan con los requisitos de la política de firma electrónica.

Tercera.- La naturaleza jurídica de la Norma Técnica de Interoperabilidad de política de firma electrónica de firma electrónica y de certificados, y de las correspondientes políticas de firma electrónica y de certificados que se aprueben, es la propia de las condiciones adicionales a la utilización de la firma electrónica en los procedimientos,

previstas en el artículo 4 de la LFE, cuya regulación ha sido complementada, y en parte, desplazada, por el RDENI y la propia Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración.

En consecuencia con lo anteriormente indicado, las reglas del RDENI, la Norma Técnica de Interoperabilidad de política de firma electrónica de firma electrónica y de certificados, y las correspondientes políticas de firma electrónica y de certificados que se aprueben, deben ser objetivas, proporcionadas, transparentes y no discriminatorias y no obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo, algo que, en nuestra opinión, no se encuentra garantizado en el texto vigente y requiere una urgente reforma.

Cuarta.- Las políticas de firma electrónica pueden ser generales o particulares, en función de las necesidades de cada organización, y las firmas generadas conforme a las mismas resultan interoperables y disfrutan del derecho de admisión por todas las Administraciones Públicas.

Dicha admisión es plena y directa cuando se emplean certificados electrónicos reconocidos y sistemas de información de revocación técnicamente compatibles con la Administración y de uso gratuito, y queda restringida a convenios de reconocimiento mutuo y recíproco en los restantes casos (incluyendo firmas basadas en certificados y otros tipos de firma electrónica), por lo que se considera necesario profundizar en la configuración jurídica de dicho escenario.

Quinta.- La admisión de sistemas de firma electrónica es, actualmente, una actuación informal de la Administración. Es necesario y urgente aprobar un procedimiento administrativo formalizado para el ejercicio del derecho de admisión en el ámbito de la Administración electrónica.

Como hemos visto al referirnos a las condiciones adicionales al uso de la firma electrónica en el sector público y a la verificación del cumplimiento de la legislación de firma electrónica como requisito para la admisión, se podría organizar esta cuestión mediante un sistema voluntario de certificación de la actividad de los prestadores que

se encuentren interesados.

Este mecanismo resultaría apropiado y equilibrado para el establecimiento de unas reglas del juego comunes para todo el territorio español, y simplificaría enormemente el ejercicio del derecho de admisión, al menos en el caso de los certificados electrónicos reconocidos.

Y por lo que se refiere a los restantes sistemas de firma electrónica, en los que ni siquiera existe un verdadero derecho de admisión ni condiciones reguladoras de su alcance, la existencia de un procedimiento formalizado resulta, en nuestra opinión, imprescindible para dotar a esta potestad de la Administración, altamente discrecional, de unas mínimas condiciones de seguridad jurídica.

Sexta.- La política de firma electrónica debe ser verdaderamente neutral en cuanto a los formatos de contenido, para no discriminar estándares abiertos ofimáticos y de amplio uso, y evitar la discriminación de los ciudadanos.

Las normas actuales no lo garantizan, no se encuentran justificadas ni en criterios de seguridad ni de proporcionalidad, ni en el Derecho europeo, que es más flexible, un aspecto que requiere de un cierto rediseño.

Séptima.- Tampoco se puede realizar una lectura completamente positiva en términos de procesos de firma electrónica: la normativa realiza una excesiva apuesta por la adopción de algunas especificaciones técnicas de formato de firma que condicionan los procesos de creación, validación y mantenimiento del valor probatorio de la firma electrónica, en perjuicio de otros mecanismos y estrategias igualmente válidos. En este sentido, puede decirse que la norma adolece de defectos importantes en cuanto a la neutralidad tecnológica.

Octava.- Resulta necesario proceder a clarificar la política criptológica referida a la firma electrónica, estableciendo reglas claras de aplicación referidas a los algoritmos a emplear en la creación, validación y mantenimiento de la firma electrónica.

La existencia de reglas de difícil engarce en la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración, en el Esquema

Nacional de Seguridad y en dos Guías contradictorias dictadas por el mismo organismo, con contradicciones y lagunas, genera mucha inseguridad jurídica en una materia de extraordinaria relevancia para la valor probatorio y la eficacia de la firma electrónica.

Novena.- La política de certificación de CertiCA, que ha normalizado todos los certificados de actuación de las Administraciones Públicas, podría reconvertirse en un conjunto de condiciones generales adicionales, a regular por reglamento, o ser parte nuclear de un sistema voluntario de certificación de la actividad de los prestadores que expiden certificados de uso en la Administración electrónica.

En nuestra opinión, continuaría siendo preciso el establecimiento de un procedimiento, pero el mismo podría contemplar la "admisión automática" cuando se verifique que el sistema empleado por el ciudadano solicitante se encuentra certificado. Para los sistemas que, cumpliendo con los requisitos del artículo 21.1 de la LAE, no se hubiese obtenido la certificación de la actividad, se debería tramitar el procedimiento completo, como hoy sucede en el caso de la admisión en el ámbito tributario.

Décima.- La Norma Técnica de Interoperabilidad actualmente sólo acepta un pequeño conjunto de todos los posibles certificados que se podrían emplear en el procedimiento administrativo: se debe, en consecuencia, estudiar con detalle la posibilidad de ampliar la política de firma para el empleo de certificados de atributos, certificados de seudónimo y certificados de representación, entre otros, y otros tipos de aserciones de identidad certificada diferentes de los certificados X.509.

Decimoprimera.- Como valoración global, se puede afirmar que la conceptualización del instrumento regulador de la utilización de la firma electrónica en el ámbito de la Administración electrónica es excesivamente complejo legalmente, con una regulación repartida y conflictiva en la LFE, la LAE, el RDLAE, el RDENI, la LUTICAJ y el futuro EJIS… y que se encuentra bastante inmaduro en términos técnicos, lo cual genera bastante retos a su adopción, y bastantes dudas sobre su legalidad.

Irónicamente, y con hemos puntualizado a lo largo de este trabajo, las especificaciones

técnicas de referencia plantean problemas de interoperabilidad relevantes, así como dificultades importantes de procesamiento automatizado, que deberán ser correctamente tratados.

Y además, nada impide que en el procedimiento de redacción y aprobación de la política de firma electrónica se incluyan condiciones adicionales incompatibles con el Derecho europeo, por lo que el test de legalidad sobre los contenidos de la política es imprescindible, y debe ser suficientemente estudiado.

Decimosegunda.- Finalmente, a medida que se incrementa la adopción de mecanismos de firma electrónica que no emplean certificados digitales, resulta necesario ampliar la regulación de las políticas de firma electrónica a dichos mecanismos, en particular dentro del marco de las denominadas federaciones de identidad, un esquema de interoperabilidad muy adoptado y perfectamente adaptable a las firmas en el sector público, y alineado plenamente con la propuesta de futura reglamentación europea de identificación electrónica y servicios de confianza para las transacciones del mercado interior.

BIBLIOGRAFÍA.

ADAMS, C. y LLODY, S. (1999): *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*, Macmillan Technical Publishing, Indianapolis.

AENOR (2007): *UNE-ISO/IEC 27001:2007 – Tecnología de la información – Técnica de seguridad – Sistemas de Gestión de la Seguridad de la Información (SGSI) – Requisitos*, Asociación Española de Normalización y Certificación, Madrid.

- (2009): *UNE-ISO/IEC 27001:2007 – Tecnología de la información – Técnica de seguridad – Código de buenas prácticas para la gestión de la seguridad de la información*, Asociación Española de Normalización y Certificación, Madrid.

AGÈNCIA CATALANA DE CERTIFICACIÓ (2011): *Política general de certificación*, en https://www.catcert.cat/esl/CATCERT/Regulacion/Documentacion-general (última visita: 27/07/2012).

ALAMILLO DOMINGO, I. (2000): "Políticas para la firma electrónica", en *Revista Seguridad en Informática y Comunicaciones (SIC)*, núm. 39, Ediciones Coda, Madrid.

- (2003): "Gestión eficaz de firmas electrónicas mediante políticas", en *Revista BoleTIC del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado*, núm. 28.

- (2011): "Política modelo de firma electrónica y seguridad documental para el sector público de Cataluña", en *Revista Seguridad en Informática y Comunicaciones (SIC)*, núm. 93, Ediciones Coda, Madrid.

- (2012): "Seguridad y firma electrónica: marco jurídico general", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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. y 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.

- (2010): "El nuevo régimen legal de gestión de la identidad y firma electrónica por las Administraciones Públicas", en COTINO HUESO, L. y VALERO TORRIJOS, J. (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*, Tirant lo Blanch, Valencia.

ARDIETA HERNÁNDEZ, J.L; GONZÁLEZ TABLAS, A.I.; RAMOS ÁLVAREZ, B. (2008): "An optimistic fair exchange protocol based on signature policies", en *Computers & Security*, núm. 27.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J.M. (2000): *La firma y el comercio electrónico en España. Comentarios a la legislación vigente*, Aranzadi, Elcano.

BAKER, S.A. y HURST, P.R. (1998): *The Limits of Trust: Cryptography, Governments and Electronic Commerce*, Kluwer Law International, The Hague.

BALLESTEROS MOFFA, L.A. (2005): *La privacidad electrónica. Internet en el centro de protección*, Tirant, Valencia.

BARRAT I ESTEVE, J. (2010): "En defensa del anonimato. A propósito de la protección de los datos personales en la actividad estadística", en COTINO HUESO, L. y VALERO TORRIJOS, J. (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*, Tirant lo Blanch, Valencia.

BASHIR, M., y KEMPF, J. (2009): "Bio-inspired reference level assigned DTW for person identification using handwritten signatures", Joint COST 2101 and 2102

International Conference on Biometric ID Management and Multimodal Communication, BioID_MultiComm 2009, *Lecture Notes in Computer Science*, Volume 5707, Springer.

BAUZÁ MARTORELL, F.J. (2002): *Procedimiento administrativo electrónico*, Comares, Granada.

BOIX PALOP, A. (2010): "Previsiones en materia de neutralidad tecnológica y acceso a los servicios de la Administración", en COTINO HUESO, L. y VALERO TORRIJOS, J. (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*, Tirant lo Blanch, Valencia.

BORGE, R.; COLOMBO, C. y WELP, Y. (2008): "Análisis explicativo de la participación ciudadana electrónica y presencial en el ámbito municipal de Cataluña", en *La democracia electrónica*, IDP. Revista de Internet, Derecho y Política, Núm. 6, UOC.

CERRILLO I MARTÍNEZ, A. (2010): "Cooperación entre Administraciones Públicas para el impulso de la Administración electrónica", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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.

COELLO DE PORTUGAL MARTÍNEZ DEL PERAL, I. (2003): "Contratos, convenios y firma electrónica", en *VV.AA.: Firma digital y Administraciones Públicas*, Instituto Nacional de Administración Pública, Madrid.

COMISIÓN EUROPEA (2010a): *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo*, COM (2010) 171 final, 20/04/2010.

- (2010b): *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Agenda Digital para Europa*, COM (2010) 245 final/2, 26/08/2010.

- (2011a): *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Acta del Mercado Único. Doce prioridades para estimular el crecimiento y reforzar la confianza. "Juntos por un nuevo crecimiento"*, COM (2011) 206 final, 13/04/2011.

- (2011b): *Comunicación de la Comisión. Hoja de ruta para la estabilidad y el empleo*, COM (2011) 669 final, 12/10/2011.

- (2012): *Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior*, COM (2012) 238 final, 04/06/2012.

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA (2010a): *Grupo de identificación y autenticación. Perfiles de certificados electrónicos*, v.1.7.6, en http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=239 (última visita: 30/07/2012).

- (2010b): *Grupo de identificación y autenticación. Política de firma electrónica basada en certificados*, v.1.8, en http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=239 (última visita: 30/07/2012).

COTINO HUESO, L. (2010): "El derecho a relacionarse electrónicamente con las Administraciones y el estatuto del ciudadano e-administrado en la Ley 11/2007 y la normativa de desarrollo", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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.

COTINO HUESO, L. y MONTESINOS GARCÍA, A. (2012): "Derechos de los ciudadanos y los profesionales en las relaciones electrónicas con la Administración de Justicia", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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.

CROBIES (2010): *Study on Cross-Border Interoperability of eSignatures (CROBIES), Guidelines and guidance for crossborder and interoperable implementation of electronic signatures*, en http://ec.europa.eu/information_society/policy/esignature/ias_crobies_studies/index_en.htm (última visita: 05/07/2012).

DUMORTIER, J., KELM, S., NILSSON, H., SKOUMA, G. y VAN EECKE, P. (2003): *The legal and Market Aspects of Electronic Signatures: Legal and market aspects of the application of Directive 1999/93/EC and practical applications of efectronic signatures in the Member States, the EEA, the Candidate and the Accession countries*. Study for the European Commission – DG Information Society, Service Contract Nr. C 28.400, Interdisciplinary centre for Law and Information Technology, Katholieke Universiteit Leuven, accesible en http://ec.europa.eu/information_society/policy/esignature/eu_legislation/index_en.htm (última visita: 29/06/2012).

ELÍAS BATURONES, J.J. (2008): *La prueba de documentos electrónicos en los Tribunales de Justicia*, Tirant lo Blanch, Valencia.

ESTEVE PARDO, J. (2010): Transparencia y legitimidad en las decisiones públicas adoptadas en entornos de complejidad científica, en GARCÍA MACHO, R. (Ed.): *Derecho administrativo de la información y administración transparente*, Marcial Pons, Madrid.

FORD, W. y BAUM, M.S. (1997): *Secure Electronic Commerce: Building the*

Infrastructure for Digital Signatures and Encryption, Prentice Hall, Upper Saddle River.

GARCÍA DE ENTERRÍA, E. y FERNÁNDEZ, T.R. (2008a): *Curso de derecho administrativo. I. Undécima edición*, Civitas Thompson, Madrid.

- (2008b): *Curso de derecho administrativo. II. Undécima edición*, Civitas Thompson, Madrid.

GARCÍA MAS, F.J. (2002): *Comercio y firma electrónicos. Análisis jurídico de los servicios de la Sociedad de la Información*, Lex Nova, Valladolid.

GRUBER, C., HOOK, C., KEMPF, J., SCHARFENBERG, G., y SICK, B. (2006): "A flexible architecture for online signature verification based on a novel biometric pen", 2006 IEEE Mountain Workshop on Adaptive and Learning Systems, SMCals 2006, IEEE.

HUERTA VIESCA, M.I. y RODRÍGUEZ RUIZ DE VILLA, D. (2001). *Los prestadores de servicios de certificación en la contratación electrónica*, Aranzadi, Elcano.

ILLESCAS ORTIZ, R. (2001): *Derecho de la contratación electrónica*, Civitas, Madrid.

INSTITUTO EUROPEO DE NORMAS DE TELECOMUNICACIONES (2002a): ETSI TR 102 041 v1.1.1 (2002-02). *Signature policies report*.

- (2002b) ETSI TR 102 038 v1.1.1 (2002-04). *TC Security – Electronic Signatures and Infrastructures (ESI); XML format for signature policies*.

- (2003a) ETSI TR 102 045 v1.1.1 (2003-03). *Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model*.

- (2003b) ETSI TR 102 272 v1.1.1 (2003-12). *Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies.*

- (2004) ETSI TS 102 280 v1.1.1 (2004-03). *X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons*.

- (2009a) ETSI TS 101 903 v1.4.1 (2009-06). *XML Advanced Electronic Signatures (XAdES)*.

- (2009b) ETSI TS 101 733 v1.8.1 (2009-11). *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*.

LESSIG, L. (2006): *Code 2.0.* Basic Books, en http://codev2.cc/ (última visita: 03/09/2012).

LINARES GIL, M. (2010): "Identificación y autenticación de las Administraciones Públicas", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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.

- (2012). "Identificación electrónica de los órganos judiciales y autenticación del ejercicio de su competencia", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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 GAMERO CASADO, E. y VALERO TORRIJOS, J. (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.

- (2012). "Identificación electrónica de ciudadanos y profesionales en el ámbito de la justicia", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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. (2009): *Administración pública electrónica*, Civitas Thompson Reuters, Cizur Menor.

- (2011). “Identificación y autenticación: DNI electrónico y firma electrónica”, en PIÑAR MAÑAS, J.L. (Dir.): *Administración electrónica y ciudadanos*, Civitas Thompson Reuters, Cizur Menor.

- (2012): “La interoperabilidad en la Administración de Justicia”, en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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 NADAL, A. (1998): *Comercio electrónico, firma digital y autoridades de certificación*, Civitas, Madrid.

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

- (2006): “Firma electrónica, certificados y entidades de certificación”, en *Revista de Contratación Electrónica*, núm. 68.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (2011): *Resumen ejecutivo del informe de la Secretaría de Estado para la Función Pública, presentado al Consejo de Ministros el 16 de septiembre de 2011, sobre la situación de la administración electrónica en la Administración General del Estado*, en http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P3401115701310558814745&langPae=es&detalleLista=PAE_13167780323707773 (última visita: 27/06/2012).

- (2012a): *Boletín de indicadores de Administración electrónica de junio de 2012*, Observatorio de Administración Electrónica, en http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P40001823013214376204 20&langPae=es (última visita: 27/06/2012).

- (2012b): *Informe CAE 2010. La Administración electrónica en las Comunidades Autónomas*, Observatorio de Administración Electrónica, en

http://www.administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P120291880134004097779 1&langPae=es (última visita: 28/07/2012).

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO y MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (2012): *Propuesta de Agenda Digital para España*, 25 de julio de 2012, en http://www.agendadigital.gob.es/ (última visita: 28/07/2012).

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA (2011): *Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración*, en http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P60215901274203521811&langPae=es (última visita: 30/06/2012).

MOLES PLAZA, R.J. (2004): *Derecho y control en Internet. La regulabilidad de Internet*, Ariel, Barcelona.

ORTEGA DÍAZ, J.F. (2008): *La firma y el contrato de certificación electrónicos*, Aranzadi, Cizur Menor.

PEPPOL (2012): *Pan-European Public Procurement Online, PEPPOL Deliverable D1.3 Demonstrator and functional Specifications for Cross-Border Use of eSignatures in Public Procurement, Part 3: Signature Policies*, en http://www.peppol.eu/peppol_components/peppol-eia/eia#ict-architecture/esignature-infrastructure/models (última visita: 05/07/2012).

PIÑAR MAÑAS, J.L. (2011): "Revolución tecnológica y nueva administración", en PIÑAR MAÑAS, J.L. (Dir.): *Administración electrónica y ciudadanos*, Civitas Thompson Reuters, Cizur Menor.

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

REGO BLANCO, M.D. (2010): "Registros, comunicaciones y notificaciones electrónicas", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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.

URIOS APARISI, X. (2012): "Los cuerpos jurídicos autonómicos y la Administración electrónica de Justicia", en GAMERO CASADO, E. y VALERO TORRIJOS, J. (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.

VALERO TORRIJOS, J. (2007): *El régimen jurídico de la e-Administración: El uso de medios informáticos y telemáticos en el procedimiento administrativo común*, Comares, Granada.

- (2008): "La gestión y conservación del documento administrativo electrónico", en BLASCO DÍAZ, J.L. y FABRA VALLS, M.J. (Eds.): *El documento electrónico. Aspectos jurídicos, tecnológicos y archivísticos*, Universitat Jaume I, Castellón.

- (2009): "Implicaciones de la protección de datos de carácter personal para la Administración electrónica", en AGENCIA DE PROTECCIÓN DE DATOS: *La protección de datos en la Administración electrónica*, Aranzadi Thompson Reuters, Cizur Menor.

VALERO TORRIJOS, J. y SANCHEZ MARTÍNEZ, D. (2007): "Protección de datos personales, DNI-e y prestación de servicios de certificación: ¿un obstáculo para la e-Administración?", *datospersonales.org*, núm. 25, en http://www.datospersonales.org/ (última visita: 24/06/2012).