Construyendo la identidad digital

Situación actual de la firma electrónica y de las entidades de certificación

Colexio Profesional de Enxeñaría en Informática de Galicia

con la colaboración de la Xunta de Galicia

Edita:

Colexio Profesional de Enxeñaría en Informática de Galicia

Colaboran:

Secretaría Xeral de Modernización e Innovación Tecnolóxica da Xunta de Galicia

Fundación para o Fomento da Calidade Industrial e o Desenvolvemento Tecnolóxico de Galicia

Lugar: Santiago de Compostela

Año de publicación: 2011

ISBN 978-84-614-6072-4

PRÓLOGO

La Xunta de Galicia entiende la Administración electrónica como un modo de ofrecer a los ciudadanos y a las empresas unos servicios públicos más eficientes y próximos mediante la utilización de las tecnologías de la información. Hoy no se concibe una Administración eficiente sin los nuevos mecanismos y dispositivos de gestión pública que proporcionan las TIC, sistemas transparentes de trabajo y servicio y la coordinación y colaboración entre los distintos niveles administrativos. Sabemos que las TIC agilizan las gestiones administrativas evitando a ciudadanos y empresas muchas cargas y desplazamientos innecesarios. No obstante, dada su gran incidencia en los procesos de modernización administrativa, tenemos que subrayar la importancia de garantizar la identidad y la confidencialidad de los trámites realizados entre los ciudadanos, las empresas y las administraciones. Es por eso que el Gobierno gallego está abordando desde esta perspectiva la mejora de su propia gestión interna en el marco de las iniciativas impulsadas por la Axenda Dixital 2014.gal.

El Consello de la Xunta de Galicia aprobó el día 2 de Diciembre de 2010 el Decreto que establece el marco de desarrollo de la Administración electrónica en la Administración pública gallega. Esta nueva norma regula, entre otros aspectos, la creación de la sede electrónica de la Xunta, la formalización del registro electrónico, la gestión digital de los procedimientos administrativos y documentos electrónicos, los medios para la acreditación de ciudadanos y empleados públicos en este nuevo contexto electrónico. El objetivo es avanzar en la mejora de la calidad y de la eficacia de los servicios ofrecidos, logrando una mayor eficiencia interna y en las relaciones intra e interadministrativas. Se trata de conseguir una Administración más transparente y abierta a los ciudadanos las 24 horas los 365 días del año.

No podemos olvidar que la Administración local es la más próxima al ciudadano. No es posible la consolidación de la Administración electrónica si no se consigue que sea una realidad también en los ayuntamientos. Es obligación de las administraciones públicas la cooperación, la coordinación, el aprovechamiento de esfuerzos y de recursos. La prestación de los servicios de acreditación digital y firma electrónica es uno de esos servicios que la Xunta pone a disposición del resto de las entidades públicas gallegas (ayuntamientos, diputaciones provinciales, universidades gallegas...) lo que les permitirá ahorrar costes para avanzar en la implantación de la Administración electrónica.

Con iniciativas como ésta, la Xunta impulsa la adaptación de la Administración autonómica a los requerimientos de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, que obliga a las administraciones a favorecer relaciones seguras y accesibles, garantizando de manera efectiva el derecho de los ciudadanos a relacionarse con la Administración por medios electrónicos.

Galicia se sitúa como la tercera Comunidad Autónoma con mayor uso de la Administración electrónica para obtener información de las páginas web y la quinta Comunidad en descarga y cumplimentación de formularios oficiales. Estos datos indican que tenemos una buena base para afrontar los cambios y los futuros retos de la Sociedad de la Información. Por eso, en la actualidad resulta

imprescindible generar confianza en las relaciones electrónicas (comunicaciones, trámites, transacciones...), contando con sistemas de acreditación, como la firma, que permitan verificar la identidad de las personas con idéntico valor que la firma manuscrita.

Resulta imprescindible difundir entre los ciudadanos y las empresas toda la información sobre el estado actual de la firma electrónica y de la certificación digital, incluyendo a las autoridades y entidades prestadoras de servicios de certificación. Es por eso que la *Secretaría Xeral de Modernización e Innovación Tecnolóxica* se congratula de colaborar con el *Colexio Profesional de Enxeñaría en Informática de Galicia* en esta iniciativa para la difusión del conocimiento existente en una materia tan sensible para el desarrollo de los nuevos productos y servicios de la Sociedad de la Información.

Santiago de Compostela, Enero 2011

Mar Pereira Álvarez

Secretaria Xeral de Modernización e Innovación Tecnolóxica

Presidencia – Xunta de Galicia

PRÓLOGO

Las últimas décadas del pasado siglo y el comienzo del presente han estado marcadas por una verdadera "Revolución Digital" debida a los cambios producidos por el impacto de las Tecnologías de la Información y el Conocimiento (TIC) en todos los ámbitos de la sociedad actual. Además, estas transformaciones se caracterizan por la velocidad a la que se incorporan a todos las esferas de nuestra vida, cambiando nuestro modo de comunicarnos, organizarnos, trabajar e incluso divertirnos.

En este proceso de cambio toma especial protagonismo Internet, como paradigma de la interconexión total. Su difusión y uso va mucho más allá de sus orígenes militares, empleándose en la actualidad de las formas más diversas que podamos imaginar: búsqueda de información, punto de encuentro, promoción personal y profesional, medio de comunicación e incluso lugar de ocio y compras.

El término Sociedad de la Información muestra, por tanto, el protagonismo que las TIC están adquiriendo en el mundo actual; pero si vamos un poco más allá, podemos comenzar a hablar de la Sociedad del Conocimiento, haciendo referencia no sólo a la capacidad de acceso a volúmenes ingentes de información sino también a la facilidad de manipulación de la misma y las posibilidades de interacción y colaboración con otras personas superando toda limitación temporal y espacial.

Es un hecho que las TIC (muchas veces llamadas, a mi entender de forma errónea, Nuevas Tecnologías, ya que el concepto de novedad conlleva una connotación de temporalidad, superada por la vertiginosidad de su evolución) están asociadas a la innovación. Cualquier nueva tecnología tiene como objetivo la mejora y superación de las características de su predecesora; sin embargo en el caso de las TIC no sólo se busca completar a las existentes, sino incluso potenciarlas y revitalizarlas.

En esta nueva sociedad, el avance tecnológico va mucho más allá de la conexión a Internet desde un ordenador. El cambio implica una evolución de los roles sociales, la cultura, el conocimiento y la información. Como ya se mencionaba antes, conocimiento e información constituyen los pilares de la sociedad del futuro.

En esta transformación tecnológica global, en la que la acumulación y manejo de la información se produce de forma masiva, las relaciones electrónicas están adquiriendo mayor presencia y relevancia. La generación de confianza en este nuevo medio de interacción tanto personal como comercial, es crucial para que llegue a todos los estratos sociales y económicos de nuestra sociedad. Es en este aspecto donde la firma electrónica está tomando más relevancia cada día.

La firma electrónica surge de la necesidad de las empresas y administraciones de reducir los costes y, sobre todo, de aumentar la seguridad de sus procesos internos. De este modo se erige como una herramienta fundamental para la mejora de la seguridad de la información y la generación de confianza, puesto que permite efectuar una comprobación de la identidad del origen y de la integridad de los mensajes intercambiados en Internet. Su condición de inmodificable aporta un grado superior de seguridad.

Este libro pretende constituirse en obra de referencia para la consulta sobre el estado actual de la firma electrónica. A lo largo del texto se va avanzando desde los conceptos más básicos relativos a la propia firma y los certificados digitales hasta una visión de futuro sobre los retos que debe abordar en cuanto a difusión, servicios y seguridad. Los diferentes capítulos van desgranando elementos fundamentales como el DNIe, los principales prestadores de servicios existentes en España, los servicios ofrecidos en relación a esta nueva modalidad de firma y la fundamental relación que se establece en torno a la administración electrónica. Se aborda además un pequeño repaso sobre cuestiones legales así como la principal normativa existente que afecta a la materia.

No se trata, por tanto, de una obra conclusa, sino que la idea es que sea actualizable en nuestro afán de convertirla en referente sobre la situación actual en todo momento sobre el uso, implicaciones y beneficios de la firma electrónica.

Desde el CPEIG somos conscientes de la relevancia que en la nueva Sociedad del Conocimiento toma la Ingeniería en Informática y de que una de sus principales funciones ha de ser la divulgativa. Es preciso extender el conocimiento de las nuevas herramientas, técnicas y normativas para hacer universal el uso de los servicios surgidos en torno a las TIC. El uso de estas implica comprender la realidad social en que se vive, afrontar la convivencia y los conflictos empleando el juicio ético basado en los valores y prácticas democráticas y ejercer la ciudadanía actuando con criterio propio. Este conocimiento y actitud contribuirá a la construcción de la paz y la democracia, y el mantenimiento de una actitud constructiva, solidaria y responsable ante el cumplimiento de los derechos y obligaciones cívicas. En definitiva, el empleo de las TIC constituye el elemento tractor fundamental para la mejora de la calidad de vida.

Santiago de Compostela, Enero 2011

Fernando Suárez Lorenzo

Presidente del Colexio Profesional de Enxeñaría en Informática de Galicia

Contenido

GRUPO DE TRABAJO

COLEXIO PROFESIONAL DE ENXEÑARÍA EN INFORMÁTICA DE GALICIA

Fernando Suárez Lorenzo

FUNDACIÓN PARA O FOMENTO DA CALIDADE INDUSTRIAL E O DESENVOLVEMENTO TÉCNOLÓXICO DE GALICIA. OBSERVATORIO DA SOCIEDADE DA INFORMACIÓN E A MODERNIZACIÓN DE GALICIA

Equipo técnico

BAHÍA SOFTWARE

Equipo de Consultoría

INTRODUCCIÓN

El objetivo principal de este trabajo es difundir entre la ciudadanía y las empresas buena parte del conocimiento existente en materia de firma electrónica y certificación digital, incluyendo las autoridades y entidades prestadoras de servicios de certificación. A este fin este estudio realiza un análisis de la situación actual, los avances más significativos y los retos que se nos presentan de cara al futuro en el ámbito de la identidad digital.

Este trabajo es fruto de la colaboración entre la Secretaría Xeral de Modernización e Innovación Tecnolóxica de la Xunta de Galicia y el Colexio Profesional de Enxeñaría en Informática de Galicia (CPEIG), a través del convenio firmado por el CPEIG y la Fundación para o Fomento da Calidade Industrial e Desenvolvemento Tecnolóxico de Galicia, en el marco de las iniciativas impulsadas por la Axenda Dixital 2014.gal.

La metodología empleada en este estudio se ha basado principalmente en la elaboración de entrevistas mantenidas con los responsables de algunas de las principales organizaciones públicas y privadas que trabajan en torno a la firma electrónica y la certificación digital, junto al análisis de datos e indicadores, legislación y documentación de referencia.

El primer capítulo ofrece una introducción conceptual al ámbito de la identidad digital.

El segundo capítulo aborda la visión estratégica de los expertos sobre los aspectos más relevantes relacionados con la certificación digital y la firma electrónica.

El tercer capítulo recoge una panorámica de los servicios y productos ofrecidos actualmente por las organizaciones, públicas y privadas, más representativas en el sector de la certificación digital y la firma electrónica en España.

El cuarto capítulo ofrece un análisis experto de la legislación existente en la materia.

El quinto capítulo hace un breve análisis de los principales indicadores estadísticos relacionados con la certificación digital y la firma electrónica.

El séptimo capítulo reúne las conclusiones.

1.

¿QUÉ ES LA IDENTIDAD DIGITAL?

La tecnología cobra cada vez más un papel más relevante en nuestras vidas y hace que poco a poco nos incorporemos a un universo tecnológico donde nuestra identidad digital transcurre paralela a nuestra identidad física.

Desde siempre la capacidad para identificar a los individuos o a las organizaciones no ha estado exenta de polémica, sin embargo hemos llegado a la utilización de sistemas consensuados y validados de identificación, como los documentos de identidad, los pasaportes, que nadie pone en duda, aún cuando existan ciertos peligros residuales en la utilización de los mismos.

En el mundo tecnológico estamos todavía en una fase temprana de identificación, de hecho podemos crear cuentas de correo electrónico gratuitas, perfiles en redes sociales, abrir blogs o *twittear* sin ningún tipo de validación sobre nuestra entidad física. Por otra parte, la mayor parte de organizaciones (como banca o *utilities*) ofrecen servicio on-line a sus clientes utilizando sistemas heterogéneos de identificación y validación.

En España desde el año 2006 se está emitiendo un documento nacional de identidad que incorpora un certificado electrónico, lo que añade un nivel de seguridad a la relación de los ciudadanos tanto con las Administraciones Públicas como con otras entidades privadas. En este caso el Ministerio del Interior actúa como tercero de confianza o autoridad de certificación.

En España, y como experiencias previas a la aparición del DNI electrónico, existe un número importante de autoridades de certificación, que emiten certificados electrónicos de diversos tipos, y funcionan como terceros de confianza en base a su cumplimiento de las garantías de acreditación que fijan tanto la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (modificada por la Ley 4/1999, de 13 de enero), como en la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos en sus relaciones con la Administración. Entre los tipos de certificados más usados están:

- Certificados individuales, referidos tanto a personas como a entidades:
    - Certificado personal, que acredita la identidad del titular.
    - Certificado de pertenencia a entidad, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
    - Certificado de representante, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
    - Certificado de persona jurídica, que identifica una empresa o sociedad como

tal a la hora de realizar trámites ante las administraciones o instituciones.

- Certificado de atributo, el cual permite identificar una cualidad, estado o situación.

- Certificados técnicos, utilizados para identificación de servidores o sistemas de información:
  - Certificado de servidor seguro, utilizado en los servidores Web que quieren proteger ante terceros el intercambio de información con los usuarios.
  - Certificado de firma de código, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.
- Certificados para Administración Pública, definidos en la Ley 11/2007, del 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos:
  - Sede electrónica, simplificando, para identificar los sitios web de las administraciones públicas
  - Sello electrónico (o de órgano), para la actualización administrativa automatizada
  - De empleado al servicio de la administración pública, para la identificación y firma de personas físicas al servicio de la administración pública

El objetivo de todo ello es proporcionar a los ciudadanos y organizaciones una identidad digital segura, que equipare su seguridad y garantías de e-ciudadano a las de ciudadano.

La Ley 59/2003 de Firma Electrónica incorpora al derecho español la normativa legal europea en materia de firma electrónica, concretamente la Directiva 1999/93/CE, por la que se establece un marco comunitario para la firma electrónica. Dicha ley regula aspectos referentes a:

- prestadores de servicios de certificación estableciendo que no está sujeta a autorización previa y se realizará en régimen de libre competencia
- DNI electrónico como medio de identificación, que acredita electrónicamente la identidad y permita la firma electrónica
- certificados electrónicos y firma electrónica reconocida
- dispositivos de creación de firma y de verificación de firma
- régimen de supervisión y control, e infracciones y sanciones

1.1. Firma electrónica reconocida

La Ley 59/2003 en su artículo 3 otorga a la firma electrónica reconocida respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los datos consignados en papel, pudiendo dar soporte a documentos públicos y privados.

Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

*1. La **firma electrónica** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.*

*2. La **firma electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.*

*3. Se considera **firma electrónica reconocida** la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.*

*4. 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.*

5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a o b del apartado siguiente y, en su caso, en la normativa específica aplicable.

6. El documento electrónico será soporte de:

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

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

c. *Documentos privados.*

Define además que una firma electrónica reconocida es considerada una firma electrónica avanzada basada en certificado reconocido, y generada mediante dispositivo seguro

de creación de firma.

Asimismo en los artículos 6 y 11 de la misma ley, se considera certificado electrónico reconocido aquel que es expedido por un prestador de servicios de certificación que cumpla los requisitos de comprobar la identidad y circunstancias personales de los solicitantes de certificados, verificar que toda la información contenida en el certificado es exacta, asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado y garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Para verificar si un certificado es reconocido se puede visitar la web del Ministerio de Industria, Turismo y Comercio donde se publican los prestadores de servicios de certificación basados en certificados reconocidos

https://www11.mityc.es/prestadores/busquedaPrestadores.jsp

Artículo 6. Concepto de certificado electrónico y de firmante.

1. Un certificado electrónico es 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.

2. El firmante es 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.

Artículo 11. Concepto y contenido de los certificados reconocidos.

1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

2. Los certificados reconocidos incluirán, al menos, los siguientes datos:

a. *La indicación de que se expiden como tales.*

b. *El código identificativo único del certificado.*

c. *La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.*

d. *La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.*

e. *La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera*

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

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

g. *El comienzo y el fin del período de validez del certificado.*

h. *Los límites de uso del certificado, si se establecen.*

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

El otro requisito que debe cumplir una firma electrónica reconocida es su generación mediante un dispositivo seguro de firma, y a ello se dedica el artículo 24 en su totalidad, indicando que los datos utilizados para la generación de la firma deben generarse sólo una vez, asegurando su secreto y protegiéndolos de forma fiable por el firmante, garantizando además que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al firmante antes del proceso de firma. Esta garantía del dispositivo debe ser emitida por entidades de certificación reconocidas tal y como se detalla en el artículo 27.

Artículo 24. Dispositivos de creación de firma electrónica.

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

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

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

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

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

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

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

Artículo 27. Certificación de dispositivos seguros de creación de firma electrónica.

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

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

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

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

Los certificados electrónicos tienen un período de validez de acuerdo con las características y tecnología empleada para su generación, y en su caso los certificados reconocidos no podrán tener un período de validez superior a cuatro años.

1.2. DNI electrónico

El Documento Nacional de Identidad ha ido evolucionando durante más de 50 años incorporando continuas innovaciones para garantizar tanto la seguridad del documento como el ámbito de aplicación. En los últimos años y con el objeto de dar cobertura a las necesidades del mundo digital ha surgido el nuevo Documento Nacional de Identidad electrónico (DNIe), que incorpora un chip capaz de guardar de forma segura información y de procesarla internamente.

Con este nuevo dispositivo somos capaces de acreditar electrónicamente y sin lugar a duda la identidad de la persona, así como de firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la firma manuscrita.

Como veíamos en el capítulo anterior el DNIe proporciona una firma electrónica reconocida, puesto que es considerada una firma electrónica avanzada basada en un certificado reconocido, emitido por el Ministerio del Interior, y generada mediante dispositivo seguro de creación de firma.

Este nuevo DNIe proporciona importantísimas ventajas sobre el DNI convencional y que podemos resumir en:

- Ampliar nuestra capacidad de actuar telemáticamente con las Administraciones Públicas, con las empresas y con otros ciudadanos.
- Realizar transacciones bancarias firmadas a través de Internet.
- Accesos a instalaciones o a sistemas informáticos.
- Realizar acciones a través de internet (compras, conversaciones,…) con garantías de que el interlocutor es quien dice ser.

Por todo lo expuesto las ventajas del DNIe son muy claras, tanto desde el punto de vista de seguridad como de comodidad, e incluso de ergonomía, puesto que físicamente es un documento más robusto y tiene una duración prevista de diez años.

2. LA OPINIÓN DEL SECTOR

El impulso que la identidad digital ha vivido en España no sería tan significativo, como lo es actualmente, sin el apoyo y la implicación de las organizaciones, públicas y privadas, que desarrollan y trabajan en las áreas de negocio, cada vez más diversas y relevantes, en torno a esta tecnología.

En las entrevistas que a continuación presentamos, mantenidas con los responsables de algunas de estas organizaciones, podemos conocer que opinan de la situación actual, de los avances más representativos y, sobre todo, de las necesidades y retos de cara al futuro.

De su experiencia y de su conocimiento podremos extraer importantes conclusiones de cara al futuro de la identidad digital, un ámbito en el que actualmente España ocupa una posición privilegiada y en el cuál se debe seguir trabajando de manera intensa para poder mantenerlo.

En este apartado se incluye además, para establecer el contexto de las organizaciones participantes en el mismo, una pequeña reseña corporativa de la historia y objetivos de cada una de ellas. Como se ha comentado ya anteriormente, aunque se han tenido en cuenta para el estudio muchas entidades y empresas, tanto públicas como privadas, para la selección de las entidades analizadas de manera más detallada se han seguidos diversos criterios de relevancia de los servicios ofrecidos, volumen de certificados gestionados o productos más innovadores.

2.1. Agència Catalana de Certificació

La Agència Catalana de Certificació (CATCert) nace el año 2002 como organismo autónomo bajo el amparo del Consorcio Administració Oberta de Catalunya. Su objetivo es proporcionar a las administraciones catalanas los instrumentos necesarios para que las transacciones electrónicas a través de Internet tengan todas las garantías jurídicas y velar para que el proceso del despliegue de la firma electrónica en la administración sea lo más amigable posible.

Las nuevas tecnologías han hecho posible la interacción y la transacción de servicios y procedimientos en línea. El impulso de las administraciones catalanas para aplicar estas tecnologías a las relaciones interadministrativas y entre administración y ciudadano, les permite ofrecer un servicio mejor y más ágil, al tiempo que supone una iniciativa innovadora en el sector público.

Una vez regulado el marco jurídico general y establecida la validez de los documentos y de las comunicaciones telemáticas, el uso de certificados reconocidos permitirá garantizar la identidad de las partes implicadas así como la confidencialidad, la integridad y el no rechazo de los documentos y las gestiones realizadas.

El conjunto de servicios ofrecido por la Agència Catalana de Certificació (CATCert) conforma el sistema público catalán de certificación.

La misión de la Agència Catalana de Certificació (CATCert) es prestar servicios de firma electrónica para las administraciones catalanas. Como tal, garantizará la confidencialidad, la integridad, la identidad y el no rechazo en las comunicaciones y transacciones electrónicas que se realicen en el ámbito de las administraciones públicas catalanas.

La Agència Catalana de Certificació (CATCert) ha establecido como principales objetivos los siguientes:

- Ofrecer a las administraciones catalanas los instrumentos necesarios para asegurar que los trámites a través de Internet tengan todas las garantías jurídicas.

- Proporcionar al personal de las administraciones catalanas diferentes tipos de certificados digitales avalados por la administración.

- Facilitar el desarrollo de aplicaciones y servicios que requieran el uso de la firma electrónica.

- Velar para que el proceso de despliegue de la firma electrónica en la administración sea lo más sencillo posible.

2.1.1. Entrevista con Xavier Tarrés Chamorro

Xavier Tarrés Chamorro

Director General

Agència Catalana de Certificació (CATCert)

Xavier Tarrés Chamorro: "La certificación digital es un avance imparable que ayuda a la modernización de la Administración Pública y conlleva una optimización de recursos fundamental para luchar contra la crisis"

El director de la Agencia Catalana de Certificación (CATCert) destaca el importante papel que tuvo el organismo como impulsor de certificados digitales y servicios de valor añadido en un momento "en que había que empezar a predicar en el desierto".

Para Tarrés Chamorro está justificada la creación de un organismo propio de certificación en Cataluña y afirma que su alcance no sólo debe medirse en clave económica, sino también en términos políticos y organizativos.

El gran reto de futuro del certificado digital es, según Tarrés Chamorro, lograr que su uso sea tan fácil y transparente que se convierta en invisible.

"Este avance imparable que suponen las nuevas tecnologías y la certificación digital ayudan a la modernización de la Administración Pública, lo que conlleva una optimización de recursos, uno de los pilares fundamentales para luchar contra esta crisis", afirma el director de la Agencia Catalana de Certificación (CATCert), Xavier Tarrés Chamorro. Para él, la e-administración es el futuro, forjado a base de los impresionantes avances tecnológicos que se ponen a disposición de la ciudadanía y también al día a día de la Administración Pública. Tal como expone, la tecnología llega a todas partes, y también a los ciudadanos, que cada vez más exigen para que la propia administración ofrezca servicios telemáticos.

De la mano de estos avances en el mundo tecnológico surge en el año 2002 la Agencia Catalana de Certificación (CATCert) como organismo autónomo bajo el amparo del Consorcio Administración Abierta de Catalunya y con la participación en un 60 por ciento de la Generalitat de Catalunya y en un 40 por ciento del mundo local a través de LocalRed. Desde su puesta en marcha tiene un objetivo claro: proporcionar a las administraciones catalanas los instrumentos necesarios para que las transacciones electrónicas a través de Internet dispongan de todas las garantías jurídicas, al tiempo que vela por el proceso de despliegue de la firma electrónica en la administración. El conjunto de los servicios ofrecidos por CATCert conforman el conocido como sistema público catalán de certificación.

Frente a los que apuestan por un modelo de unidad en materia de autoridad de emisión de certificaciones digitales, el máximo responsable de CATCert defiende la propuesta catalana que tuvo, según apunta, "un papel de impulso importante, tanto a nivel de certificados como de servicios de valor añadido", especialmente en un -momento –en el que nació- que todavía no había mercado, ni regulación, ni necesidades. "Había que empezar a predicar en el desierto", recuerda.

"El momento en que se constituye CATCert creo que fue una decisión muy acertada", asegura Xavier Tarrés Chamorro, quien explica que, aunque económicamente se ha gastado más dinero frente a la alternativa de *outsourcing* de servicios, esta inversión ha hecho que la situación actual en Cataluña sea "mucho más avanzada que en otras comunidades por impulso del conocimiento, por capacidad independiente de dirigir las políticas de administración electrónica o por nivel actual de implantación, entre otras". "La aceptación de CATCert como autoridad permite estar fuertes en el despliegue de la e-administración en Cataluña", apunta Tarrés Chamorro.

En este punto, el responsable de CATCert explica que la evolución en materia de certificación digital ha supuesto que su entidad haya pasado de moverse en un mercado de oferta (sólo CATCert y FNMT ofrecían servicios a las administraciones) a un mercado de demanda, ya que ahora son las propias administraciones locales y autonómica las que cada vez más solicitan una cartera de servicio más amplia y con acuerdos de nivel de prestación de servicios muy exigentes.

La Agencia Catalana de Certificación tiene un triple rol. Tal como explica su director, es una autoridad prestadora de servicios de certificación como tercero de confianza, según los dictados de la ley de firma electrónica, que además ofrece servicios de valor añadido que ayudan a utilizar, extender y fomentar la identidad digital y la firma electrónica. Además, el organismo ofrece servicios de acompañamiento y asesoramiento con el objetivo de que la brecha digital se reduzca lo antes posible. Con este encargo CATCert se estructura de manera interna en tres áreas clave: área de certificación y calidad; área técnica; y área de asesoría e innovación.

Rentabilidad futura

Consultado sobre el retorno de la inversión realizada en la puesta en marcha de una autoridad de certificación propia en Cataluña Xavier Tarrés Chamorro lo tiene claro: "El retorno de la inversión es muy difícil de calcular", pero recalca que la rentabilidad de esta iniciativa no debe medirse únicamente en términos económicos. En este punto, hace referencia a la situación actual que se vive en la comunidad, con una economía a escala; con una estrategia de administración electrónica fuerte y que mantiene la identidad propia; con una red coordinada con protocolos y ritmo de despliegue propios; y en la que la cooperación entre administraciones se ve reforzada con una posición fuerte para aplicar los servicios de identidad y documento electrónicos, en especial cuando se tienen calendarios propios

y coordinados entre todas las administraciones de la Comunidad. Para él esto hace ver que el retorno de la inversión realizada en el CATCert "es político, en el sentido de que es consecuencia de una decisión estratégica que es ganadora seguro".

Según los datos que maneja Tarrés Chamorro, hasta el momento CATCert ha emitido ya cerca de 160.000 certificados de ciudadano, otros 60.000 de empleado público y más de 1.500 de servidor o dispositivo, con los servicios necesarios que estos llevan asociados. El presupuesto anual del organismo asciende a los 5 millones de euros y cuenta con un equipo compuesto por 31 personas.

Usos del certificado digital

Según apunta el director del CATCert, existe una diferencia importante entre Europa y España en el uso del certificado digital ya que, mientras que en Europa el motor de promoción de esta tecnología ha sido la banca, en España ha sido la Agencia Tributaria. Además, destaca la labor "muy importante" de impulso del certificado electrónico en Cataluña realizado desde las cámaras de comercio y desde el entorno profesional. Aún así, para Tarrés Chamorro el papel clave lo juega, sin lugar a dudas, la Administración Pública, tanto por volumen de trabajadores públicos y de necesidades de automatización certificada como por su papel de tractor de empresas y ciudadanía. "Si la administración ofrece servicios importantes para el usuario a través de la web seguro que el ciudadano va a utilizarlos", apunta, al tiempo que recuerda que también los jóvenes ocupan un papel relevante en este impulso, "por su visión y capacidad tecnológica y porque ya empiezan a ocupar puestos relevantes y con poder de decisión en las empresas".

Para Xavier Tarrés Chamorro "el mercado del certificado digital es todavía incipiente, a pesar de que nuestro país cuenta con una veintena de prestadores. La alfabetización digital –escasa- de nuestra población, las dificultades de comprensión de estas tecnologías y el estado todavía incipiente de la "vida digital" de los negocios y las transacciones en el entorno de Internet, hacen necesaria una optimización de las aplicaciones de cara a un uso "amigable y compatible con todos los sistemas". También que la oferta de certificados a la población final pueda extenderse de forma masiva. "Es un pez que se muerde la cola".

Concretamente en el caso de CATCert, Tarrés Chamorro recuerda que el organismo presta servicios de certificación a las Administraciones Públicas y también ofrece certificados digitales para los ciudadanos, el equivalente al que emite la Fábrica Nacional de Mercado y Timbre (FNMT). Por el contrario, CATCert no ha orientado sus servicios a las empresas "para no interferir en un mercado libre que ofrece ya servicios y que está los suficientemente maduro".

Legislación digital

En lo referente a la situación legislativa actual en materia de certificación digital Xavier Tarrés Chamorro se muestra contrariado. Según explica las leyes actuales han supuesto la eliminación de barreras e imponen una serie de retos en materia de certificación digital, "pero siempre respecto a la obligación de la administración". Así, a su juicio los derechos de los ciudadanos reconocidos en la Ley 11/2007, del 22 de junio, que obliga a la Administración Pública a poner todos los servicios ofrecidos en Internet todavía no son los suficientemente conocidos y entendidos a nivel ciudadanía. "Serán las nuevas generaciones las que realmente los demanden", considera, en un futuro en el que sí se reconocerá el papel pionero de España en el reconocimiento de los derechos del ciudadano a través de Internet.

A pesar del importante avance que supone esta ley, en ella no se abordan los procesos automatizados que una operación de esta magnitud debe llevar asociados, según explica Tarrés Chamorro. A pesar de esto, alaba el hecho de que la normativa "ponga la alfombra a la gestión de identidades, al documento electrónico con garantías jurídicas, al archivo documental, en definitiva, a la vía digital". "La vía digital de la Administración Pública tiene que evolucionar sincronizando caminos tan diversos como el tecnológico, el de regulación y el de procedimientos", añade.

Para Tarrés Chamorro la legislación, que antes era una de las grandes barreras a la administración electrónica y al uso de certificados digitales como infraestructura básica de esta e-administración, ya no es hoy en día un impedimento para los avances digitales sino más bien un impulso. En la actualidad las barreras a la administración electrónica vienen impuestas por la usabilidad de las propias tecnologías y por el cambio cultural y de hábitos que esta nueva administración requiere.

Al concretar la aplicación de la Ley 11/2007, del 22 de junio, en Cataluña, Xavier Tarrés Chamorro considera que en estos momentos Generalitat y ayuntamientos grandes y medios se encuentran en la fase de despliegue de la normativa, avanzando claramente a una consolidación de la misma. Por el contrario, son los pequeños ayuntamientos los que se encuentran en una posición más retraída. En este punto, recuerda que existe una estrategia de infraestructura definida por la propia Generalitat para llevar la banda ancha al medio rural, favoreciendo así la implantación de los servicios digitales en los municipios con mayores dificultades. Para Tarrés Chamorro es una estrategia necesaria porque la implantación electrónica necesita ir a la par de la implantación de infraestructuras.

En este punto Tarrés Chamorro aportó la innovadora experiencia puesta en marcha en Cataluña, donde se ha emitido una normativa que obliga a los ayuntamientos a enviar electrónicamente sus cuentas y actas de gobierno. Un total de 947 administraciones locales han comenzado ya a operar con este sistema, que funciona a través de una plataforma intermedia y que supone el uso de certificaciones digitales, con la total validez jurídica que conlleva y el ahorro de tiempo, intermediarios, errores, archivo físico y gastos de transporte.

Retos de futuro

El futuro pasa por la tecnología, por la aplicación de las tecnologías a los procesos de gestión de los servicios públicos. Pero aunque el certificado digital se presente como una de las grandes soluciones tecnológicas de las próximas generaciones, sin la cual no es posible desplegar la vía digital, para el director de la Agencia Catalana de Certificación es necesario tener en cuenta problemas como la preservación de la firma electrónica en el tiempo, puesto que es de obligado cumplimiento mantener su continuidad y validez. Para ello, explica, CATCert ha desarrollado una plataforma de gestión documental con un sello de perdurabilidad que aborda estas necesidades. Este puede ser uno de los muchos retos a los que se enfrenta el mundo digital. "A medida que avanzamos nos encontramos con nuevos problemas en esta vida digital que iniciamos", reflexiona Xavier Tarrés Chamorro.

En esta línea, Tarrés Chamorro aborda igualmente el objetivo principal del organismo que dirige. Su finalidad es seguir desarrollando su trabajo actual, sin intención inicialmente de convertirse en proveedor de servicios para otras comunidades y otros organismos fuera de Cataluña, "porque podría interpretarse como una competencia del ámbito empresarial". Saber gestionar esta premisa con éxito es, para Tarrés Chamorro, la clave para evitar conflictos de intereses con las entidades privadas, garantizando la pervivencia futura de ambos tipos de organismos. Otro tipo de colaboración interadministrativa para la mejora o aceleración en la implantación de sistemas de certificación digital siempre es posible.

Además, es consciente de que la implantación definitiva del DNIe supondrá, a medio o largo plazo, el fin de los certificados de ciudadano que CATCert emite actualmente. "En España tenemos la gran suerte de contar con la ayuda del DNIe de cara al ciudadano, aunque necesita mejorar su usabilidad", subraya. Este es, sin duda, el gran reto al que se enfrenta la certificación digital de cara al futuro: conseguir que el uso de los certificados digitales sea tan fácil y transparente que se haga invisible para el ciudadano.

Sobre la situación de España en materia de certificación digital en contraste con Europa, Xavier Tarrés Chamorro recuerda que el marco legislativo es común, aunque afirma que los servicios de interoperabilidad todavía deben evolucionar. En este sentido se ha trabajado a nivel europeo en el proyecto STORK, para conseguir el reconocimiento paneuropeo de las identidades electrónicas; y a nivel español en la creación de una línea TSL´s, o listas de confianza interoperables entre estados miembros. "Pero es un camino a largo plazo", detalla. Además, recuerda que desde Europa se identifican a las infraestructuras de identidad digital como herramientas clave para salir de la crisis, una gran oportunidad pero a la vez un gran reto para los países.

Por otra parte, según Tarrés Chamorro, para España es muy importante, desde el punto de vista económico, ser interoperables con países de Latinoamérica, "puesto que son vías de negocio para los

proveedores de servicio españoles".

"La oportunidad de cara al futuro es que la vía digital está creciendo, y es necesario ofrecer soluciones de acuerdo a las necesidades que están creciendo", concluye Xavier Tarrés Chamorro, confiado en las posibilidades de España, como país, de hacer frente a los grandes retos a los que se enfrenta ya en la era digital.

2.2. Albalia Interactiva

Albalia Interactiva es una empresa de Consultoría y Servicios, de capital español, creada en 1997, con experiencia en entornos de alta tecnología bancarios y de telecomunicaciones.

Entre sus especializaciones están la seguridad, firma electrónica, factura electrónica, administración electrónica, banca electrónica, medios de pago y movilidad.

El enfoque seguido es de "Tecnología Legal". Es decir, Albalia lleva a cabo un intenso seguimiento de todos los avances legislativos que tienen implicaciones tecnológicas en el ámbito tanto de las entidades financieras como en otros tipos de empresas en los que este enfoque sea significativo. De esta forma se descubren interesantes posibilidades que pueden ser aprovechadas por las entidades más avanzadas o más preocupadas por el servicio al cliente y, en otras ocasiones, se identifican normas que implican obligaciones para las entidades, lo que se engloba en las necesidades de "*Compliance*" o cumplimiento normativo.

Albalia Interactiva desarrolla proyectos de Hacking Etico, mystery shopping, Factura electrónica, UBL, XBRL, Firma electrónica, Mobipay, DNI digital, PDF inteligente, Voto electrónico, LOPD-LSSI, UNE 71502, ISO 17799, UNE 166001 y 166002, e-notario créditos personales, e-notario hipotecario, tarjetas inteligentes, PKI, Single Sign On, Evidencias Electrónicas y Análisis Forense.

2.2.1. Entrevista con Julián Inza Aldaz

Julián Inza Aldaz

Presidente

Albalia Interactiva

Julián Inza: "Nuestro valor añadido fundamental es la seguridad jurídica que aportamos en todos los procesos con documentos digitales"

El presidente de Albalia Interactiva destaca como peculiaridad de la compañía la sinergia con empresas del grupo, en función de las acciones que realiza: de consultoría, de formación y de desarrollo de productos y servicios.

Para Inza la complejidad de las implementaciones prácticas del uso del DNI electróni-

co están retrasando el cambio esperado respecto al desconocimiento o indiferencia de la ciudadanía ante la certificación digital.

La seguridad jurídica que ofrece Albalia Interactiva en todos los procesos en los que pueda aplicarse la firma electrónica y certificación digital es, según el presidente de la entidad, Julián Inza, el valor añadido fundamental de la marca. El grupo de consultoría y servicios relacionados con la certificación digital y las nuevas tecnologías nace en 1997, como Librería Interactiva. En 2003 se crea Albalia Interactiva, enfocándose en la consultoría técnica y jurídica y en el desarrollo de soluciones de seguridad, y la Librería Interactiva se transforma en Atenea Interactiva, la empresa del grupo especializada en formación. Albalia se especializa en la seguridad, firma, factura, administración, comercio y banca electrónica, así como en medios de pago y movilidad. En 2009 nace EADTrust, la tercera empresa del Grupo, como PSC, Prestador de Servicios de Certificación. Especialmente desde 2003 su perfecto conocimiento de la ley y de su aplicación ha sido la clave de la empresa, que ofrece a sus clientes y usuarios esa seguridad jurídica en todas sus acciones. Además, otro valor que ofrece la compañía es su trabajo como consultora y auditora en digitalización certificada para empresas que desean homologar sus soluciones ante la Agencia Tributaria. El proceso crea documentos digitales a partir de los de papel y con su mismo valor. O, en otros contextos, es posible crear documentos que nacen de forma electrónica preservando el máximo valor probatorio, incluso en instancias jurisdiccionales centradas en la presentación de pruebas en formato papel. “Podemos garantizar que un documento electrónico bien gestionado iguala y supera en valor probatorio a un papel”, explica Julián Inza.

Una de las peculiaridades del Grupo Interactiva es su organización estructurada en función de las acciones que realiza. De este modo, Albalia se centra en la consultoría, auditoría y prestación de servicios; Atenea Interactiva se orienta a la formación; y EADTrust, es un PSC que usa y comercializa en forma de servicios, los productos desarrollados por Albalia. Según explica el presidente de la compañía, el conocimiento y formación que ofrece Atenea se centra especialmente en los campos de la factura, firma y administración electrónicas, además de abordar cualquier novedad legal relacionada directa o indirectamente con la certificación digital. La extensa e intensa labor de investigación que desarrolla esta organización permite después aprovechar sus avances en materia de auditoría y consultoría en Albalia. Por su parte, EADTrust trabaja en el campo del “timestamping” para completar la firma electrónica; en la publicación fehaciente del perfil del contratante; en la custodia de documentos electrónicos; en la notificación fehaciente y en el voto electrónico. Así, Julián Inza apunta que el Grupo tiene dos maneras de enfocarse al cliente: como consultora, que aporta algunos productos tecnológicos de confianza digital, a través de la firma Albalia y como prestador de servicios de eConfianza en la nube TIC a través de EADTrust.

El enfoque de Albalia Interactiva es de tecnología legal, es decir, desde la empresa se realiza un intenso seguimiento de todos los avances legislativos que tienen implicaciones tecnológicas en el ámbito de las entidades financieras, de las administraciones públicas y de otro tipo de empresas en los que

este enfoque sea significativo. De esta forma se encuentran posibilidades interesantes que pueden ser aprovechadas por las entidades más avanzadas o más preocupadas por el servicio al cliente, al tiempo que se identifican normas que implican obligaciones para las entidades, lo que se engloba en las necesidades de cumplimiento normativo.

Usos del certificado digital

Respecto al uso de la certificación digital el presidente de Albalia Interactiva lo tiene claro, es la Administración Pública "la que está tirando del carro" y donde más se ha impulsado esta nueva tecnología. "Los ciudadanos todavía no son conscientes de la versatilidad de la firma electrónica", asegura Julián Inza, quien considera que la Administración Pública esta siendo el tractor que impulsa el desarrollo de esta tecnología y de otras conexas, como la custodia digital representada por la sede electrónica y el código localizador CSV (código Seguro de Verificación). De hecho, para Inza la lenta adopción de estas nuevas tecnologías entre la ciudadanía se explican también por la forma tan compleja con la que los implementadores de soluciones como el registro electrónico o los sistemas de interlocución telemática tratan al DNIe, que provoca el rechazo o indiferencia de la población ante esta nueva tecnología. "Hay que hacerlo más sencillo para el usuario, Con los medios actuales se pueden evitar fallos exasperantes o tareas repetitivas sin valor" insiste Inza.

En esta línea, Julián Inza apunta a otros campos donde el uso del certificado digital será interesante y tendrá gran importancia en el futuro, como son la banca, la sanidad, la universidad y las empresas denominadas "de utilities", es decir, que ofrecen servicios de telecomunicaciones, luz, agua o gas, entre otros. Son las entidades con las que los ciudadanos interactúan frecuentemente y están obligadas a disponer de sistemas de "interlocución telemática" o a garantizar el derecho de los ciudadanos a relacionarse con ellas por medios electrónicos.

Consultado sobre la transición del mundo del papel al mundo electrónico, el presidente de Albalia Interactiva explica que hasta el momento el mecanismo básico de la gestión de la firma está sustentado en "parábolas" digitales del mundo físico, donde el paradigma es el formato PDF, "y prácticamente lo poco que se ha hecho en el sector privado es la firma de ficheros PDF". Así, recuerda que estos documentos en PDF tienen muchas carencias, que los del mundo del papel no tienen, y es que dependen del concepto de documento original, que no existe en el mundo digital sino como convencionalismo. Y es que, según explica Inza, cuando tienes un papel original ese documento tiene una serie de cualidades que lo trascienden: la obliterabilidad; la endosabilidad y la completitud. En los documentos electrónicos esas cualidades se desvinculan del concepto de original y se gestionan separadamente con sistemas de custodia digital y una definición inteligente de los metadatos adecuados, más próxima a la gestión informática transaccional, que a la documental.

En este contexto hay que señalar el significado de estos términos. La obliterabilidad, implica la posibilidad de que un documento represente un derecho y deba quedar registrado si se ha hecho uso o no del derecho. Por ejemplo, un billete de autobús se cancela al montar en el autobús y no se puede reutilizar en el futuro. La endosabilidad, implica la posibilidad de transferir a otro el derecho que refleja un documento, algo relativamente fácil de gestionar en los documentos nomnativos y más complejo en los documentos al portador. El ejemplo típico es el de la letra de cambio o los títulos valores (acciones). La completitud, es la capacidad de añadir anotaciones al margen, en los espacios libres o añadiendo hojas, o incluso reflejando elementos de otros documentos. Un ejemplo es el de un contrato que refleje la existencia de un anexo posterior, o un poder en el que se anote posteriormente que se ha revocado, y se asocie a una inscripción registral

Para Inza, cuando sólo queremos dar certeza de que un documento se ha firmado entre las partes un PDF es un documento válido. Por ello estamos viendo que el paso del mundo del papel al electrónico y viceversa, por ejemplo en el ámbito de la compulsa, se está empezando a realizar través del PDFs firmados. Pero admite que en el ámbito privado todavía falta un mecanismo que permita a los particulares ejercer el derecho a la prueba cuando se trata de su intervención en documentos electrónicos, que sí pueden gestionar los organismos e instituciones que ponen en marcha los sistemas de relación telemática. En este sentido Inza destaca la interesante propuesta puesta en marcha por el Gobierno Vasco, denominada Metaposta. Según su opinión, esta iniciativa puede evolucionar en un futuro hacia un sistema de correos electrónicos con mecanismos de custodia o puede convertirse en un dispositivo para centralizar las evidencias de los firmantes, "un modelo muy valioso". La dificultad, para Julián Inza, es que los ciudadanos "todavía no han interiorizado lo que supone una firma electrónica en el ámbito público y/o privado".

En este punto, Julián Inza recuerda que el modelo electrónico de gestión de documentos requiere dos instrumentos: la firma electrónica y la custodia digital. Según explica, la custodia digital es exigente y compleja, ya que requiere la certeza la protección de la información a largo plazo, y su disponibilidad ante instancias jurisdiccionales, lo que exige la implantación de mayores mecanismos de seguridad; e implica la responsabilidad de organismo relacionado con la autenticidad del documento, de ahí el concepto de sede electrónica. Los documentos requieren un control riguroso de metadatos que reflejan la traza de anotaciones o vinculaciones a identidades o a otros documentos para garantizar la obliterabilidad, la endosabilidad y la completitud. "La custodia digital es más compleja de gestionar que la firma electrónica que, aunque también tiene su complejidad, es una materia en la que todos tenemos más experiencia", apostilla.

En lo referente a la introducción del certificado digital en el día a día de los ciudadanos el presidente de Albalia Interactiva considera que son "las generaciones jóvenes las que realmente fomentarán el uso del certificado digital de manera habitual". A pesar de esta optimista perspectiva de futuro, Inza

también es consciente de que todavía "queda un tiempo para madurar" y reconoce que hoy en día sólo las personas que tienen la obligación o necesidad de utilizar el documento digital en su día a día lo hacen.

Documento notarial electrónico

En lo referente al documento notarial electrónico el presidente de Albalia Interactiva explica que esta tecnología está contemplada tanto en el actual reglamento notarial, cuya modificación ha sido muy reciente, en 2007, como en la Ley de Acompañamiento de los presupuestos del año 2002, Ley 24/2001. Así, explica que este documento está pensando para determinadas comunicaciones que se realizan entre notarios y registros, "que es donde tienen su mayor virtualidad". En esta línea también se enmarca el concepto de protocolo electrónico, que ofrece los parámetros básicos de cómo se debe hacer una custodia de un documento digital, "porque los conceptos de cosido y de índice del protocolo son los mismos que, aplicándolo al mundo electrónico permiten la buena llevanza de la custodia digital". Además, en este proceso, tal como recuerda Julián Inza, los notarios, jueces y secretarios judiciales son figuras clave a la hora de entender qué es un documento electrónico, ya que son los profesionales del ámbito jurídico que más claramente entienden el significado de este documento y sus elementos básicos.

A efectos prácticos actualmente todavía no se puede solicitar en una notaría una copia autorizada firmada electrónicamente, salvo para su traslado a otro notario, a un registrador o una administración pública, aunque sí una copia simple, si el notario aprecia interés legítimo, y esta posibilidad existe desde finales del año 2001. Es una cuestión que, para Julián Inza, necesita todavía un tiempo para su implantación, aunque destaca el hecho de que a día de hoy "todos los notarios de España disponen de la firma electrónica reconocida".

Legislación europea

El presidente de Albalia Interactiva es tajante en materia de legislación y afirma rotundo que existe un déficit "muy grande" en la Unión Europea procedente de la mala aplicación del artículo 11 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, por la que se establece un marco comunitario para la firma electrónica. En este artículo se exige a los países miembros la comunicación a la Comisión Europea del estado de supervisión de los prestadores de certificación digital de su ámbito. A pesar de esta obligación, Julián Inza lamenta que no se especificase de manera clara la estructura de la información a suministrar, lo que ha provocado que cada país lo defina de manera unilateral y envíe posteriormente la documentación a la Comisión Europea. De hecho, apunta que dos cuestiones clave en la información a suministrar serían el certificado root de la autoridad de certificación y el lugar

donde consultar la validez de los certificados, el servicio OCSP (Online Certificate Status Protocol). Además, critica que, once años después de emitir esta directiva, se publicasen los protocolos TSL (Trust-service Status List), que deberían haber servido para facilitar el cumplimiento de la normativa y la elaboración de un listado común de prestadores de servicio, pero que, muy al contrario todavía mantienen carencias básicas, ya que, por ejemplo, no incluyen información sobre los servicios de validación de cada uno.

La falta de concreción de la normativa europea ha provocado que actualmente no exista un listado común de todos los prestadores de servicios de certificación digital de Europa, sino un simple listado de países y, dentro de cada uno y en sus respectivos idiomas, las indicaciones de cómo encontrar cada uno de los prestadores en sus propias páginas web. Para Inza sería necesario disponer de un listado normalizado para que las herramientas, por ejemplo los navegadores, tengan el camino más fácil para buscar la información de prestadores de confianza y de la validez de cada uno de sus certificados emitidos y redunde en una mejor experiencia del usuario.

En esta línea, el máximo representante de Albalia Interactiva apunta a una alternativa a esta iniciativa de la Unión Europea, y que consistiría en una plataforma para acceder a la lista de certificados revocados de una manera sencilla. En esta cuestión "España es pionero y está dando un ejemplo a seguir", a lo que ayuda el hecho de que sea el país con más prestadores de servicios de certificación de la Unión Europea y, después de Estados Unidos, el que más prestadores de servicios de certificación tiene registrados en los navegadores.

Marco legislativo español

"El entorno de legislación español está mucho más desarrollado que el de la mayor parte de otros países de nuestro entorno, es uno de los mejores de Europa en estos momentos", expresa el presidente de Albalia Interactiva, al tiempo que concreta que este marco legislativo está muy por delante del de los países anglosajones, y no tanto de los países de origen latino, donde la necesidad de la firma electrónica está más clara y asumida. Aún así, matiza que, a pesar de que hay un "buen nivel" en cuanto a cantidad de normativa referente a certificación digital, se debería mejorar en lo referente a calidad. "Haría falta desarrollar más los conceptos del documento electrónico, incidiendo en la sistemática del documento", apunta Julián Inza. Además, lamenta la descompensación legislativa que existe para el sector público, con mayor normativa, y para el sector privado, con menor detalle en las leyes que imponen el uso de la firma electrónica.

Comunidades autónomas y certificación

Consultado sobre la decisión de determinadas Comunidades Autónomas de convertirse en entidades

de certificación o prestadores de servicios de certificación digital, el presidente de Albalia Interactiva destaca con rotundidad la actitud que Andalucía ha tomado al respecto. A pesar de no contar con una autoridad de certificación digital, a su juicio, Andalucía ha entendido bien la problemática de la gestión documental electrónica, más allá de la relevancia que puede tener entre sus organismos un prestador de certificación propia o no.

Por otra parte, para Julián Inza el peso que la identidad propia tiene en el ámbito de las competencias es lo que ha llevado a comunidades como País Vasco, la Comunidad Valencia o Cataluña a desarrollar autoridades autónomas de certificación digital. En este aspecto Inza considera que en España existen iniciativas y experiencias "muy interesantes", así como profesionales altamente cualificados al frente de estas entidades autónomas. Sin embargo, considera que lo más importante no es la capacidad para prestar servicios de certificación, sino la capacidad de gestionar documentos electrónicos con los servicios de certificación que ya existen, "y ahí la labor más notable ha sido la que ha desarrollado la Administración Pública andaluza".

Retos de futuro

El presidente de Albalia Interactiva ve como "casi imprescindible" el hecho de que en el futuro todas las Administraciones Públicas dispongan de mecanismos de gestión de documentos electrónicos y de ayuda en el despliegue de la administración electrónica. En lo referente a la convivencia de las entidades públicas y privadas de certificación digital, Julián Inza considera que el modelo de negocio de la Fábrica Nacional de Moneda y Timbre (FNMT) debería cambiar y permitir el acceso sin coste a la información de certificados revocados, lo que implicaría también un cambio en su mecanismo de financiación. Por ejemplo, cree que un cambio estratégico sería incluir a CERES transitoriamente como parte de la infraestructura del Ministerio de Política Territorial y Administración Pública, lo que le proporcionaría un valor añadido muy importante a un ministerio que, según destaca Inza, "está haciendo una labor muy interesante en su responsabilidad de dinamizador de la modernización administrativa y en la apertura del mercado de la certificación".

"A largo plazo tendría sentido que desaparecieran las iniciativas públicas de expedición de certificados digitales", apunta también Julián Inza, quien considera que las necesidades de gestión de identidades digitales de carácter público se cubrirán con el DNIe, que permitirá gestionar la mayor parte de las necesidades de identificación a nivel personal. En este punto, Inza explica que en España existen en la actualidad en torno a 26 prestadores de servicios de certificación privados y públicos, por lo que "sería interesante plantearse si es necesario financiar con presupuestos públicos iniciativas que tienen suficiente respuesta por parte del sector privado, que por su parte se encuentra en condiciones de competencia desvirtuada por las iniciativas públicas".

En este punto, el presidente de Albalia Interactiva considera que el principal reto del futuro digital es terminar con el problema de la interoperabilidad de las firmas electrónicas en Europa, lo que se alcanzaría mediante la adopción generalizada de formatos basados en XML; el uso de firmas XADES-XL; la inclusión de anclas de confianza, de los certificados root de los PSC y URL de los servicios de consultas de revocación de los PSC en las TSL´s; y la codificación correcta del campo de consulta de certificados revocados por parte de los prestadores de servicios de certificación. Y en esta misma línea, sería también necesario abordar el problema de la interoperabilidad de los documentos electrónicos, un reto a su juicio "muy difícil" cuya solución pasaría por crear un repositorio sincronizado de formularios XML donde todos los formatos sean subidos por su creador y modificados por los usuarios que los utilicen, si detectan carencias.

Unido a esta perspectiva de futuro digital, el responsable de Albalia Interactiva reconoce que actualmente la implantación real de la factura electrónica es otro de los grandes retos a los que se enfrenta el campo de la certificación digital y un avance tecnológico que supondría importantes mejoras de eficiencia para las empresas.

Albalia ante el futuro

Desde su creación, Albalia Interactiva se plantea como reto ir un paso por delante en materia de certificación digital. Así, en el plan estratégico de futuro la compañía está trabajando la idea de crear un sello de calidad para el ámbito de la digitalización de firmas manuscritas, con el que distinguir soluciones que merecen o no confianza, de tal forma que se audite el sistema y avalen las soluciones de gestión documental que asocian firmas digitalizadas que cumplan ciertos principios, como la imposibilidad de reutilizar las firmas capturadas por parte de las entidades que las captan, con tabletas digitalizadoras o por otros procedimientos..

Además, entre las labores de Albalia Interactiva, Julián Inza plantea la necesidad de estudiar de qué forma se recogen las evidencias para que la firma digital tenga el valor que le otorga la ley, porque "cualquier firma digital no es válida". "El problema es que los usuarios no saben distinguir cuando hay por detrás sistemas que ofrecen confianza o no", lamenta.

"La Administración Pública está haciendo esfuerzos para inculcar en el ciudadano esa forma de ejercer sus derechos a través de la tecnología, y el sector privado podrá subirse a la ola y beneficiarse de ello", concluye Inza.

2.3. Camerfirma

AC Camerfirma, S.A. fue creada en el año 1999, como un proyecto cameral con el objetivo de dotar de seguridad a las comunicaciones y operaciones telemáticas realizadas en el ámbito empresarial. Actualmente la compañía está participada por el Consejo Superior de Cámaras de Comercio, por más de 85 Cámaras de Comercio españolas y por el grupo Banesto. Además, formamos parte de CHAMBERSIGN, entidad supranacional de ámbito europeo, que otorga reconocimiento a nuestros certificados más allá del territorio nacional.

Se establece como prestador de servicios de certificación al amparo de la LEY 59/2003, de 19 de diciembre, de firma electrónica, es decir como tercero de confianza en las transacciones electrónicas, distribuyendo certificados de identidad que permiten a las empresas identificarse en la red y firmar electrónicamente documentos con total seguridad técnica y jurídica.

AC Camerfirma es un prestador reconocido para la emisión de certificados a las Administraciones Públicas en base al desarrollo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Desde el comienzo de su trayectoria como sociedad anónima en el año 2000, mantiene una estrecha relación con los mercados de Sudamérica y cuenta en su labor con numerosos proyectos de consultoría y de implantación de PKI con las Cámaras de Comercio sudamericanas (Cámara de Comercio Uruguay, Cámara de Comercio de Bogotá, Cámara de Comercio de Chile,…). A partir de este año 2009, Camerfirma ha empezado además la realización de proyectos de implantación de PKI en países de Europa como Portugal, Grecia,…

2.3.1. Entrevista con Rafael Román Álvarez

Rafael Román Álvarez

Responsable de Administraciones Públicas

Camerfirma

Rafael Román Álvarez: "El punto fuerte de Camerfirma es nuestra amplia red cameral con la que dar un buen servicio y asesoramiento a empresas y administraciones públicas"

El responsable de Administraciones Públicas de Camerfirma destaca el hecho de que

la entidad disponga de 88 oficinas de registro con cerca de 600 personas con capacidad para generar certificaciones digitales.

Para Román Álvarez uno de los hechos que diferencia a su entidad de cualquier otra emisora es la validez internacional de sus certificados digitales.

"Nuestro valor añadido es la amplia red cameral que tenemos para dar servicio a todas las empresas y administraciones públicas. Nuestro punto fuerte es darles un buen servicio y asesoramiento, que cuando compren sepan lo que compren", subraya determinante Rafael Román Álvarez, el responsable de Administraciones Públicas de Camerfirma. Ese es el objetivo y el principal motivo de la creación, en el año 1999 de AC Camerfirma, un proyecto cameral que nace para dotar de seguridad a las comunicaciones y operaciones telemáticas realizadas en el ámbito empresarial. En la actualidad la compañía está participada por el Consejo Superior de Cámaras de Comercio y forma parte, además, de CHAMBERSING, una entidad supranacional de ámbito europeo que otorga reconocimiento a sus certificados digitales más allá del territorio nacional.

El valor diferencial de Camerfirma es, sin duda, la amplia red de oficinas de registro basadas en las cámaras de comercio de las que disponen, un total de 88 actualmente, y las cerca de 600 autoridades de registro con las que cuentan en toda España, es decir, aquellas personas con capacidad para generar certificados digitales. Esta red de recursos se teje con el único y principal objetivo de dar el mejor servicio y asesoramiento a sus clientes. Para ello Camerfirma trabaja con un soporte en tres niveles: un nivel uno basado en las preguntas básicas de los usuarios; un segundo para la integración de firmas digitales con productos; y el tercero, de sistemas, orientado al desarrollo de productos. Además, otro valor que diferencia a Camerfirma de cualquier entidad similar es su carácter y validez internacional, porque la validez de sus certificados digitales se otorga a través de las cámaras de comercio, organizaciones que existen en todos los países del mundo.

Oportunidad de negocio

Camerfirma se establece como prestador de servicios de certificación al amparo de la Ley 59/2003, del 19 de diciembre, de firma electrónica, es decir, como tercero de confianza en las transacciones electrónicas, distribuyendo certificados de identidad que permiten a las empresas identificarse en la red y firmar electrónicamente documentos con total seguridad técnica y jurídica. Además, es prestador reconocido para la emisión de certificados a las Administraciones Públicas en base al desarrollo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Según explica Rafael Román Álvarez ahora Camerfirma está tratando de extenderse a otros países, al igual que lo está haciendo la Fábrica Nacional de Moneda y Timbre (FNMT), abriendo nuevos mercados, como en Méjico donde se utiliza la certificación digital para los trámites con la oficina de

registro de la propiedad. “Estamos abriendo nuevos mercados, y en algunos sitios ya lo hemos hecho”, apunta.

Aún así, a corto plazo y de manera más cercana la principal oportunidad de negocio que tiene Camerfirma es trabajar con la Administración Pública, para la implantación de todos los nuevos sistemas. “Hasta ahora se están poniendo los certificados justos para poder ponerlos en marcha, supongo que a partir del año que viene se terminará de consolidar toda la administración pública”.

En lo referente a las empresas la apuesta es clara: el certificado digital para el mundo empresarial, fomentándolo a través de las cámaras de comercio. Además, también hay cabida en este proyecto de futuro para las novedades, como el bussines wear, con el que permitir a las empresas avanzar en soluciones propias con firma digital. “Para nosotros también es una prioridad ofrecer productos de firma y factura electrónica, y estamos trabajando en ello”, concluye.

Usos de la certificación digital

Sobre los ámbitos actuales de uso de la certificación digital, el responsable de Administraciones Públicas de Camerfirma considera que hasta ahora se limitaba al mundo empresarial, en trámites con Hacienda o la Seguridad Social, pero hoy comienza a extenderse a la Administración Pública “y cuando realmente esté implantado será la que tire por ese uso del certificado digital”. “Y esperemos que empiece a tirar también del ciudadano y del uso del DNIe” apunta. Además, Román Álvarez añade que cuando la Administración Pública termine de implantar todos sus sistemas, sus sedes electrónicas o la factura electrónica, entre otros, será el momento en que se obligue a sus proveedores a usar certificados digitales y a los ciudadanos a usar el DNIe, una situación que, a su juicio, no se producirá antes de un par de años.

En lo referente al uso concreto de la firma digital, para Román Álvarez es una técnica poco desarrollada actualmente en el mundo empresarial, aunque espera que despunte con la facturación electrónica, cuando la Administración Pública la tenga implantada y empiece a exigirla. “Hoy por hoy en el mundo empresarial el certificado digital se conoce y se usa sólo para tramitaciones con la Administración Pública”, sentencia. En este sentido, explica que desde Camerfirma se han desarrollado productos para fomentarlo, como son los portales de facturación electrónica para pymes y micropymes o los bussinesswhere, productos con soluciones de firma asociadas.

En este punto, se matizan las diferencias entre el certificado digital y la firma electrónica. Mientras que el certificado digital es un documento digital mediante el cual un tercero confiable – una autoridad de certificación – garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública; la firma digital es aquella firma reconocida y almacenada en un soporte electrónico y que tiene el mismo valor legal que la manuscrita.

Para el responsable de Administraciones Públicas de Camerfirma uno de los principales motivos del poco uso de la firma electrónica y del certificado digital se debe al desconocimiento que hay de sus posibilidades y garantías, tanto a nivel empresarial como en la ciudadanía. "El ciudadano como ciudadano tiene un gran desconocimiento de la firma digital y de las tramitaciones que puede hacer", lamenta Román Álvarez, quien, aún así, reconoce el esfuerzo que están haciendo algunas comunidades autónomas para informar a la ciudadanía en estos aspectos.

En este sentido, considera que el primer paso debería ser ayudar a la empresa privada, a la Administración Pública y la ciudadanía a distinguir sobre los distintos tipos de certificados digitales: los emitidos por la FNMT, con uso limitado a los trámites con las Administraciones Públicas; los certificados empresariales, emitidos por entidades privadas, que son certificados de atributos para el mundo empresarial y sirven para firmar documentos como persona perteneciente a una entidad, vinculando al trabajador a esa empresa con un cargo determinado en la misma; y el DNIe, para firmar documentación como ciudadano. "Hay que enseñar para qué es cada tipo de certificado digital", apostilla.

Certificado digital y legislación

A juicio del responsable de Administraciones Públicas de Camerfirma en materia legislativa sobre certificación digital "tenemos la ley, pero todavía no hay conceptos demasiado claros, por lo que su aplicación es diversa". Por ello, explica que las empresas optan por desarrollar sus productos según su criterio. Además, reconoce que la crisis actual está provocando una ralentización en esta materia, siendo las empresas y las Administraciones Públicas las que "tienen más complicado ponerse al día con la ley".

Por otra parte, se aborda también la situación actual tendente hacia la homologación europea y mundial en materia de certificación digital. Tal como explica Román Álvarez, los certificados camerales otorgados por Camerfirma tienen valor internacional, pero todavía a día de hoy hay países que están fuera de este acuerdo. "Nuestra validez se da a través de las cámaras de comercio, y en todos los países hay una cámara de comercio. Esa es la que da legalidad a nuestra firma", detalla Román Álvarez, quien considera que es este punto donde se encuentra uno de los puntos fuertes de la empresa. "Nuestra validez internacional es una de las grandes diferenciaciones respecto a otras entidades de certificación digital", sentencia de manera contundente.

Comunidades autónomas como entidades de certificación

Para el miembro de Camerfirma el hecho de que varias comunidades autónomas españolas se conviertan en entidades de certificación digital no es algo negativo, siempre y cuando tengan una orientación global y emitan documentos que sirvan para realizar tramitaciones en cualquier otra comunidad.

Acerca de la implantación de la Ley 11/2007, de firma electrónica, Rafael Román Álvarez entiende que es un proceso muy lento ya depende de una serie de actuaciones que éstas deben realizar y que se encuentran paralizadas debido a la negativa coyuntura económica actual. "La firma electrónica es la guinda del pastel", apunta, al tiempo que explica que sólo una vez que las Administraciones Públicas tengan implantados todos sus procesos electrónicos en Internet se podrá cerrar el proceso con la implantación generalizada del certificado digital, con el que poder realizar la firma electrónica en todas estas tramitaciones.

El futuro digital

Consultado sobre la convivencia en un futuro de las entidades públicas y privadas de certificación digital, el responsable de Administraciones Públicas de Camerfirma opina que a largo plazo únicamente se utilizarán los certificados de empleado público, que permitirán la supervivencia de las entidades de certificación privadas y las comunidades autónomas; y los certificados de atributo o empresariales, para dar capacidad de firma a las empresas y organizaciones; y el DNIe. "Todavía queda por venir algo nuevo, no sé muy bien qué, pero el DNIe tiene que irse mejorando para mejorar la impresión del usuario", matiza. En este sentido, recuerda que para el ciudadano el DNIe tiene como principal reto extender su conocimiento y uso, además de necesitar superar las complicaciones técnicas que todavía implica su uso en la actualidad.

2.4. Cuerpo Nacional de Policía - DNI electrónico

El Documento Nacional de Identidad electrónico es el documento que acredita física y digitalmente la identidad personal de su titular y permite la firma electrónica de documentos.

Su apariencia es similar al DNI actual, al que se incorpora un chip electrónico, que contiene la información básica que permita acreditar electrónicamente la identidad de su titular y la firma de documentos electrónicos con plena validez legal.

La principal ventaja del DNI electrónico frente al convencional es que además de identificar al usuario ante terceros, permite la firma electrónica. El nuevo DNI aporta seguridad, rapidez, comodidad y la inmediata realización de trámites administrativos y comerciales a través de medios telemáticos.

El chip que incorpora el DNI electrónico contiene los mismos datos que aparecen impresos en la tarjeta (filiación, fotografía y firma digitalizada y resumen criptográfico de la impresión dactilar) junto con los certificados de autenticación y firma electrónica, además de un certificado de componente propio del DNIe. El nuevo DNI no contiene ningún dato histórico del titular como tampoco incorpora dato alguno de carácter sanitarios, fiscal, penal, laboral,…

2.4.1. Entrevista con Juan Crespo Sánchez

Juan Crespo Sánchez

Inspector Jefe

Área de Informática

Cuerpo Nacional de Policía

Dirección General de la Policía

Juan Crespo: "La Administración Pública española ha apostado por el desarrollo de las TIC, y esto ha facilitado que seamos referentes en aspectos como la identidad digital"

El inspector jefe del Cuerpo Nacional de Policía destinado en el área de Informática destaca la importancia del DNIe, que comenzó a emitirse en el año 2006, convirtiendo a España en el cuarto país de la Unión Europea que disponía de este novedoso dispositivo.

El reto actual del DNIe es lograr que todas las aplicaciones que lo usan sean certificadas, para transmitir así a los ciudadanos una sensación y realidad de seguridad a todos los niveles.

En el año 2006 se materializa, como proyecto piloto, una iniciativa con la que la Administración pública española pretende avanzar en la sociedad de información dotando a los ciudadanos de un documento de identidad electrónico: el DNIe. Los primeros pasos se remontan al año 2000, cuando el Gobierno pone en marcha el proyecto INFO XXI para el desarrollo de la sociedad de la información, en el que se analizan los aspectos relacionados con la seguridad de los nuevos servicios telemáticos. Es entonces cuando se determina la necesidad de crear un documento de identidad electrónico con el que dotar a los ciudadanos de un mecanismo que les permita realizar transacciones electrónicas e interactuar de manera segura, así como realizar procesos de firma e identificación electrónica. El elemento común a todos los ciudadanos era el Dni, por lo que se optó por desarrollarlo en una nueva versión con la que lograr un documento válido tanto para la identificación física como para la electrónica.

Para Juan Crespo, inspector jefe del Cuerpo Nacional de Policía del área de Informática, esta apuesta de la Administración Pública española por el desarrollo de las TIC "ha facilitado que seamos referentes en aspectos como la identidad digital". En este éxito no sólo se incluye al DNIe, sino también todo el trabajo realizado por diversas entidades de certificación y al desarrollo de los servicios relacionados necesarios por parte de la Administración Pública y las entidades privadas. Así, hoy en día se pueden realizar a nivel local, autonómico y estatal diferentes transacciones electrónicas cuya garantía está avalada por el uso del DNIe y de otros certificados similares. Estos avances facilitan a los ciudadanos múltiples posibilidades en las tramitaciones, con ahorro de tiempo y costes.

España comenzó a trabajar en el proyecto del DNIe en el año 2001 y la experiencia piloto de expedición de documentos electrónicos se concreta en el año 2006, implantándose de manera definitiva dos años más tarde. También en el año 2006 se empieza a expedir, de manera única y exclusiva, el nuevo pasaporte electrónico. Este documento incorpora como novedad un chip de radiofrecuencia que garantiza que los datos impresos no han sido alterados y que coinciden con los del chip. Sin embargo, el pasaporte electrónico funciona únicamente como elemento identificativo y carece de capacidad de firma.

"Hemos sido de los primeros países en incorporar esta tecnología a la sociedad", subraya Juan Crespo en referencia al DNIe. Esta apuesta de España por la certificación digital se puso de manifiesto cuando comenzó a emitirse el DNIe, momento en el que sólo existían experiencias similares en Finlandia, Bélgica y Estonia. Actualmente hay cerca de 10 países inmersos en este proyecto, siendo Alemania el último en incorporar documentos de identificad electrónicos, concretamente en noviembre del pasado año.

DNIe como elemento dinamizador

"El DNIe no tiene vocación de ser exclusivista, sino que nace con vocación de elemento dinamizador y facilitador de la sociedad de información y de los servicios de certificación digital", detalla el responsable Seguridad para los Sistemas Informáticos del área de Informática del Cuerpo Nacional de Policía. Así, explica que la Ley 59/2003, del 19 de diciembre, de Firma Electrónica permite la expedición de otros certificados de firma electrónica basados en un registro hecho con un certificado ya expedido. El DNIe permite la generación de nuevos prestadores de servicios de certificación sin necesidad de que desplieguen oficinas de registro. Esto se realiza en base a un registro que puede realizarse por Internet, siempre y cuando se utilice un DNIe u otro certificado que esta normativa defina como documento reconocido. Además, el nuevo certificado heredaría la fortaleza del certificado en base al cual se hace ese registro telemático. "Eso lo que permite es la proliferación de prestadores de servicio virtuales", añade, al tiempo que asegura que con este mecanismo se optimizan y se reducen los costes de una infraestructura y logística de servicios de certificación, la parte más difícil de asumir por parte de las empresas prestadoras de servicios de certificación digital.

Consultado por la implantación actual de la certificación digital, Juan Crespo explica que desde la Administración Pública se han desarrollado diversas acciones para impulsar el uso de los servicios telemáticos basados en certificados electrónicos. En este sentido destaca tres medidas clave: el propio DNIe como elemento de firma electrónica de los ciudadanos; la Ley 11/2007, del 22 de junio, que obliga a la Administración Pública a dotarse de los medios y sistemas electrónicos que posibiliten a los ciudadanos a ejercer su derecho a comunicarse con las Administraciones por medios electrónicos; y la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, con la que se obliga a las empresas que prestan servicios básicos a los ciudadanos a gestionar dichos servicios a través de Internet.

En este sentido, ha sido la Administración Pública la que más ha apostado por el desarrollo de todos los servicios y usos asociados a la certificación digital, por lo que está "plenamente integrado" en este ámbito. Sin embargo, en el sector privado no se ha adquirido todavía el mismo nivel de implantación.

Percepción y seguridad del DNIe

En lo referente a la percepción del DNIe por parte de la ciudadanía el inspector jefe del Cuerpo Nacional de Policía del área de Informática es tajante: "No existe un conocimiento demasiado amplio de todo lo relacionado con esta tecnología por parte de los ciudadanos, a pesar de las campañas de formación y sensibilización llevabas a cabo por la Policía, el Ministerio de Industria, el INTECO o el proyecto Red.es, entre otros". Así, considera "importante difundir y hacer llegar a los ciudadanos las

bondades y la seguridad que ofrece el DNIe", entre las cuales destaca el hecho de que este documento asegura la identidad del portador, evitando cualquier tipo de suplantación de la misma en una operación.

En esta línea, hay que recordar que la seguridad de la operación que se realiza a través del DNIe radica en la entidad que ofrece el servicio, responsable de prestar servicios seguros. Para ello en colaboración con el Ministerio de Industria, el INTECO, Red.es y el Centro Criptológico Nacional se han elaborado de forma conjunta una serie de guías de uso de las aplicaciones que emplean el DNIe, así como una serie de perfiles de protección. El objetivo es que las aplicaciones que utilizan el DNIe se puedan certificar contra esos perfiles de protección, pudiendo así garantizar a los ciudadanos que dichas aplicaciones son totalmente seguras. "Que cuando firmas algo no hay suplantación del documento que tú estás firmando", matiza.

A este respecto, subraya que desde el Cuerpo Nacional de Policía no sólo se certifica como seguro el chip del DNIe, sino que además actualmente se está procediendo a certificar conforme a la ISO 27001, el estándar internacional aprobado en 2005 en el que se recogen los requisitos para establecer, mantener y mejorar un sistema de gestión de la seguridad de la información. El reto ahora es lograr que las aplicaciones que hacen uso del DNIe estén también certificadas, para transmitir así a los ciudadanos una sensación y realidad de seguridad a todos los niveles. "Desde mi punto de vista como ciudadano me gustaría que todas las aplicaciones que use sean certificadas, porque es la única manera de garantizar que estoy haciendo una operación segura", recalca Juan Crespo.

Usos del DNIe

El Cuerpo Nacional de Policía ha emitido hasta el momento más de 20 millones de DNIe, lo que supone que más del 50 por ciento de la población española dispone de este documento (teniendo en cuenta que los menores de 14 años no tienen obligación de estar identificados a través del Dni). A pesar del gran porcentaje de población que cuenta con este dispositivo y, aunque al emitirlo se ofrece al titular documentación informativa sobre sus usos, todavía existe una limitación en cuanto a edad, formación y disponibilidad de banda ancha a la hora de hacer un correcto uso del DNIe. Por ello, aún hoy en día no se han alcanzado los niveles óptimos de funcionalidad de este documento electrónico.

En este punto, el inspector jefe del Cuerpo Nacional de Policía recuerda que la firma electrónica con DNIe tiene consideración de firma manuscrita y le da plena operatividad en el ámbito de Internet. Pero a pesar de los avances conseguidos a través de este documento el mundo de las nuevas tecnologías es imparable y "siempre estamos en constante evolución", por lo que siempre aparece algún detalle que permite mejorar el dispositivo. Así, "actualmente se está trabajando en el diseño y construcción del próximo chip para adaptarse a la evolución tecnológica, prestando especial atención a

las normas internacionales y a la seguridad", detalla.

En esta línea, Juan Crespo explica que la liberalización de los comando APDU facilita la proliferación o generación de aplicaciones, ya que permite que cada organización pueda generarse su propio interfaz de acceso al DNIe. "Es igual de seguro, puesto que siempre va a requerir el PIN del ciudadano, pero es más sencillo puesto que se podrán definir su propio interfaz y los comandos de acceso a bajo nivel dentro de sus aplicaciones", señala. Esto permite, por ejemplo, incluir en los cajeros automáticos de los bancos los accesos al DNIe sin que ello sea un proceso de adaptación tecnológica costosa para la empresa.

Interoperabilidad en el mundo electrónico

Con el objetivo de garantizar su interoperabilidad el DNIe se ha adaptado a la normativa europea e internacional existente. Para ello, antes de diseñar el proyecto del nuevo documento electrónico España se sumó a distintos grupos de trabajo a nivel europeo, como el proyecto EPOCH, que definía una serie de normas de interoperabilidad. Desde entonces los avances han sido muchos y muy diversos, por lo que España sigue participando en otras iniciativas con las que mantenerse al día en esta materia. Así, actualmente España, a través del Ministerio de Política Territorial y Administración Pública, participa enel proyecto STORK, que persigue la interoperabilidad electrónica en la Unión Europa y en el que participan organizaciones españolas tanto públicas como privadas. Como ejemplo del trabajo desarrollado por España, Juan Crespo explica que precisamente a este grupo se le han enviado los comandos APDU para que sean incluidos en un middleware común que se está construyendo con el fin de validar todas las tarjetas de identidad electrónica europeas.

Para garantizar la interoperabilidad del DNIe España también ha trabajado a una escala inferior, pero no por ello menos importante. Así, hay que destacar los acuerdos formalizados con Portugal para el reconocimiento mutuo de los certificados electrónicos de los documentos de identidad entre ambos países. Todo ello con la colaboración del Ministerio de Política Territorial y Administración Pública que mediante su plataforma @firma, valida los certificados digitales portugueses para su uso en España.

Retos de futuro

Tal como reconoce Juan Crespo, la situación económica actual ha supuesto un freno importante en este tipo de iniciativas tecnológicas, ya que se trata de proyectos que requieren una inversión considerable y cuya rentabilidad no puede medirse a corto plazo. "Hay que adaptar todos los procedimientos físicos al mundo electrónico, y eso requiere un coste", reconoce. Además, el hecho de que los proyectos que se realicen deban garantizar su compatibilidad tecnológica en el futuro supone un

incremento de los costes, lo que limita las inversiones en esta materia. “Existen una serie de costes ocultos que irán apareciendo conforme se materialicen estas necesidades, a nivel de custodia electrónica, por ejemplo”, avanza.

A pesar de la coyuntura económica, los avances realizados en materia de certificación digital han puesto de manifiesto la necesidad de acortar los plazos de vida del soporte físico para igualarlo al electrónico. De hecho, una paradoja actual es el hecho de que el soporte físico tiene una validez que puede llegar a los diez años, mientras que la Ley de Firma Electrónica establece que el período máximo de vida de un certificado electrónico debe ser de cuatro años, lo que requiere una sincronización de la renovación física y la renovación electrónica.

Otro de los retos de futuro pasa por la necesidad de crear un documento de identidad electrónica para los extranjeros, a los que actualmente no se les proporciona certificados de identidad ni de firma electrónica. Así, en este momento una persona de nacionalidad extranjera debe acudir a una entidad privada para solicitar un documento de este tipo. El único avance realizado en este sentido se materializará a partir de este verano, cuando las tarjetas de identificación de extranjeros incorporen un chip de radio frecuencia, similar al del pasaporte electrónico, que permita verificar que no ha sido manipulada la parte física. Pero este sistema tendrá única y exclusivamente validez para la identificación presencial, por lo que todavía habrá que avanzar al respecto.

En este sentido, los proyectos actuales de pasaporte electrónico y la futura tarjeta de identificación electrónica de extranjeros son “decisiones comunitarias, homogéneas, compatibles e interoperables al cien por cien dentro de la Unión Europea”. Además, el nuevo pasaporte electrónico tiene una parte compatible e interoperable con el resto de los países que conforman la Organización Internacional de Aviación Civil.

También en materia de servicios asociados a la certificación electrónica se presentan nuevos e importantes retos. “Un reto para la Administración Pública es ofrecer servicios de calidad a los ciudadanos”, asegura Juan Crespo, al tiempo que explica que para el Cuerpo Nacional de Policía ofrecer el DNIe no supone solamente expedir el documento y los certificados electrónicos alojados en el mismo, “sino ofrecer servicios de alta disponibilidad, como son las listas de certificados revocados, servicios que faciliten a los prestadores de servicios de validación el acceso a dichas listas y mantener los servidores en línea las 24 horas del día los 7 días de la semana”.

2.5. FirmaProfesional

Firmaprofesional nació en el año 2001 como un proyecto de diversos colegios profesionales con el fin de actuar con total independencia como Autoridad de Certificación Digital de los Profesionales. Inicia su actividad en enero de 2002, es un operador global de servicios de certificación y proveedor tecnológico de seguridad y confianza, ofreciendo al mercado su especialización y experiencia, entre otros, en los ámbitos de tecnología, seguridad y normativa legal.

Es una de las empresas pioneras en España como Autoridad de Certificación, emite certificados digitales especializados tanto para los profesionales, sus colegios y colectivos, como para las empresas y sus empleados y genera sobre ellos una serie de servicios de valor añadido para el mercado.

Los certificados digitales de persona física y persona jurídica que emite Firmaprofesional son Certificados Reconocidos, pero para determinados proyectos en entornos cerrados de usuarios Firmaprofesional también comercializa Certificados para Firma Electrónica Avanzada.

2.5.1. Entrevista con Santiago Núñez Mella

Santiago Núñez Mella

Responsable de Cuentas

FirmaProfesional

Santiago Núñez Mella: "Nacemos con un objetivo claro: cubrir las necesidades de los colegios profesionales en materia de certificación digital"

El responsable de Cuentas de Firmaprofesional destaca la vocación de una entidad que desde 2001 ha sabido atender de manera eficiente la demanda de los colectivos profesionales de toda España.

La adaptación a las necesidades del cliente, el eficiente sistema de soporte y mantenimiento y la especialización en el ámbito de colegios profesionales son, a juicio de Núñez Mella, los puntos claves del éxito de la empresa.

Cuando en el año 2001 echa a andar Firmaprofesional lo hace con un objetivo claro: cubrir las necesidades de los colegios profesionales, faltos hasta el momento de un certificado digital específico que

les identificase como personas físicas adscritas a un colectivo profesional. Según explica el director de Cuentas de Firmaprofesional, Santiago Núñez Mella, hasta entonces ninguna Autoridad de Certificación emitía certificados de colegiado, se limitaban a certificados digitales de persona física o a certificados de atributo para colegios profesionales que carecían de la suficiente funcionalidad. Núñez Mella lo deja claro: "Nacemos con un objetivo claro: cubrir las necesidades de los colegios profesionales en materia de certificación digital".

Pero Firmaprofesional no se limita a emitir certificados digitales para colegios profesionales y va más allá creando autoridades de registro en estos colectivos, de tal manera que ellos mismos son autónomos para mantener todo el ciclo de vida del certificado. Todo este sistema de certificación digital resulta en el año 2001 "novedoso y muy idóneo para estos colectivos profesionales" y supone dejar en mano de los propios colegios profesionales su gestión en materia de certificación digital ya que, tal como apunta Núñez Mella, son ellos los que tienen el mejor conocimiento y control de su colectivo.

Aunque la andadura de Firmaprofesional se inicia como un proyecto de diversos colegios profesionales con el fin de actuar con total independencia como Autoridad de Certificación Digital de los profesionales y se orienta en un primer momento exclusivamente a las necesidades específicas de los profesionales y de las entidades que los agrupaban, en la actualidad ha ampliado su campo de actuación y ofrece servicios de certificación tanto a corporaciones públicas y privadas como a empresas.

Así lo explica el responsable de Cuentas de Firmaprofesional, quien afirma que fruto de la experiencia con los colegios profesionales se amplía el accionariado de la empresa con nuevas entidades como la patronal de la pequeña y mediana empresa de Cataluña, orientándose Firmaprofesional a servicios más globales, como consultoría estratégica o factura electrónica, entre otros.

Retos de futuro

El futuro de la firma está claro: "Exportar la experiencia a otros países". Así, el reto fundamental al que se enfrenta Firmaprofesional día a día es seguir implantando y concienciando acerca de las bondades del uso del certificado digital, tanto en Administración Pública como en la empresa privada. "Es necesario concienciar del beneficio y del ahorro de costes, algo de lo que ya se han dado cuenta muchas empresas, aunque también hay otras muchas que no lo utilizan", explica Núñez Mella.

"Queremos poder y saber transmitir, hacer una eficiente labor de comunicación para que la gente aborde este tipo de proyectos", continúa. Además, se centra en sus declaraciones en la importancia que la investigación y los avances tecnológicos tienen en este campo concreto, por lo que su firma apuesta por seguir haciendo I+D+I para disponer de nuevos productos y servicios con los que adelantarse a la normativa y facilitar a sus clientes todos los trámites posibles con valor añadido.

Productos y servicios

Es necesario diferenciar dos tipos de actuaciones dentro de Firmaprofesional, por un lado se diferencian los productos, en los que se incluyen los propios certificados digitales; la comercialización de los dispositivos donde se almacenan estos certificados de manera segura (tokens, tarjetas criptográficas...), ya que el 98 por ciento de los certificados emitidos van en dispositivos seguros de creación de firma; y las plataformas de firma. Por otra parte habría que detallar los servicios: de sello de tiempo, conocido como timestamping; de validación de otros certificados de forma gratuita; y de consultoría y definición de procedimientos.

Acerca del valor añadido que ofrece Firmaprofesional a sus productos y servicios frente a otras autoridades de certificación digital, el responsable de Cuentas de la firma lo tiene claro: "la adaptación que nosotros hacemos al cliente, adaptamos la solución y la personalizamos en función del cliente. Además, estamos especializados en colegios profesionales, trabajamos con más de 80 en toda España". Y junto a estas dos claves en su día a día, no hay que olvidar la "eficiente" ayuda que Firmaprofesional presta al cliente en soporte y mantenimiento, en incidencias funcionalmente básicas pero técnicamente complejas. De hecho un estudio realizado el pasado año por su empresa revela un alto grado de satisfacción del cliente en materia de atención y servicio.

Uso de certificado digital

La certificación digital está extendida desde hace años en los colegios profesionales de España, con técnicos visadores que utilizan la firma electrónica y con colectivos que usan este sistema electrónico para visar, evitando cada vez más el uso del papel. Además, Núñez Mella destaca el hecho de que cada vez más la Administración Pública ponga a disposición de la ciudadanía un mayor número de servicios telemáticos, con el consiguiente avance tecnológico y de beneficios para el ciudadano.

El uso de la certificación digital es, para Santiago Núñez Mella, un avance porque supone ahorro de tiempos, de costes y de logística pero que al mismo tiempo ofrece unos niveles de seguridad más elevados. "La firma electrónica no sólo garantiza la identidad, sino la integridad, ya que el documento no se modifica desde que la persona lo ha firmado", detalla. De hecho, se refiere al DNIe como un dispositivo seguro que facilita al ciudadano la realización de trámites con total seguridad, al tiempo que "crea cultura del uso de certificados digitales de cara a la empresa, viendo los beneficios que conlleva ofrecer operaciones telemáticas". El aspecto negativo de este avance es la escasa información que se ha ofrecido a la ciudadanía sobre su uso lo que, unido a la falta de lectores de tarjeta para el DNIe, ha provocado el desconocimiento y desinterés de esta tecnología por parte de la población. "La crisis económica tampoco está ayudando a que las empresas se aventuren a acometer nuevos proyectos para avanzar en el uso del DNIe, porque la rentabilidad se vería a medio plazo", apostilla.

En este aspecto, se lamenta que ni empresas ni ciudadanos sean conscientes de los beneficios que estos avances en materia de certificación digital tienen para su día a día. "Este proceso de implantación requiere su tiempo", reconoce, citando como ejemplo el proceso de implantación que tuvo en su día la telefonía móvil. En este punto, considera Núñez Mella que la Administración Pública debería actuar como catalizador de los cambios tecnológicos, como por ejemplo ocurre en Galicia con la factura electrónica, ya que todos los proveedores deben integrarse en un sistema para facturar de manera telemática.

A pesar de encontrarse en este punto de inflexión, el miembro de Firmaprofesional subraya que "en el ámbito de identidad digital España está a la cabeza, un ejemplo es el proyecto del DNIe, pionero en Europa". Este liderato supone que ahora otros países que comienzan en esta aventura digital tengan a España como referencia, aprovechándose del conocimiento generado con la experiencia española.

Situación legal

Consultado sobre el marco legal de la certificación digital, el responsable de Cuentas Santiago Núñez Mella es tajante: "Existen leyes pero no todo está suficientemente claro". Tal como explica, se dictó la Ley 59/2003, del 19 de diciembre, pero teniendo en cuenta la progresión de los avances tecnológicos es un marco legal que se queda desfasado. "A veces hay una aplicación un tanto laxa de la ley para facilitar la introducción de esta tecnología", señala Núñez Mella, quien considera que además debería existir un régimen sancionador que favoreciese la aplicación de la misma.

A nivel europeo, desde Firmaprofesional se reclama la necesidad de disponer de un órgano intermedio que actúe de enlace entre todos los países y sus entidades de certificación digital, una cuestión en la que ya se está trabajando. Además, Núñez Mella es firme en su opinión de considerar a España como un ejemplo en materia de certificación digital: "La experiencia que tenemos en España deberíamos intentar exportarla, y cuanto antes mejor", se reafirma.

También Santiago Núñez Mella aborda los motivos que llevan a una comunidad autónoma a convertirse en entidad de certificación digital o prestadora de servicio, algo que, a su juicio no resulta necesario, "sino más bien es una ausencia de optimización de recursos". "Deberíamos tender a proyectos más globales", añade, al tiempo que recuerda que crear una autoridad de certificación "es muy costoso, por lo que no veo lícito que para financiar ese retorno de la inversión las entidades de comunidades autónomas compitan en dar servicio a administraciones públicas autonómicas o locales frente a otros proveedores de servicio privados, ni que publiquen concursos públicos que limiten la participación de proveedores de servicio privados". Además, matiza que, en cualquier caso los sistemas deberían ser interoperables aceptando así los certificados de cualquier entidad homologada por el Ministerio de Industria.

Certificado digital: nexo de unión

Para el responsable de Cuentas de Firmaprofesional el futuro de la certificación digital pasa porque tanto las entidades públicas como privadas de certificación tiendan al uso del DNIe para evitar tener que acreditar su condición de profesional o asociado, entre otros. En esta punto diferencia por una parte la labor realizada desde la Fábrica Nacional de Moneda y Timbre (FNMT) quien, según su criterio, "ha hecho bien su trabajo", pero aún así la ciudadanía desconoce que la emisión del certificado digital es gratuito para el ciudadano pero no lo es la validación para la entidad pública o privada, algo que, tal como apunta Núñez Mella, estas entidades no ven con buenos ojos.

Por ello, a su juicio, el DNIe desplazará estos certificados, lo limitará la existencia de la FNMT como autoridad certificadora únicamente para la Administración Pública, trabajando de manera exclusiva en la emisión de certificados de funcionario, sede electrónica y sello electrónico.

"Entidades públicas y privadas tenderán en un futuro al uso del DNIe" recalca Santiago Núñez Mella, quien apunta que el uso de este documento se complementará a nivel profesional con el certificado profesional, que cubrirá las necesidades de profesionales y asociados. Como ejemplo, cita la implantación de la telefonía móvil, con dos usos distintos y complementarios: el móvil personal y el móvil profesional, cada uno con sus fines particulares.

En este punto entran en valor los servicios prestados por Firmaprofesional que, según detalla el responsable de Cuentas de la firma, son económicamente más competitivos respecto a entidades como la FNMT, "quien debe tener unos costes más razonables, más cuando se financia con fondos públicos".

2.6. FNMT-CERES

La revolución de la tecnología de información, conjuntamente con el desarrollo de la infraestructura de comunicaciones, está haciendo cambiar significativamente las relaciones entre individuos y organizaciones, tanto en España como en todo el mundo. Estas nuevas formas de comunicación abren un gran abanico de posibilidades tanto para ciudadanos como para empresas y permiten comercializar productos y servicios de una forma ágil y económica.

En España, las distintas Administraciones están apostando decididamente por Internet como vía de comunicación, creando webs con información de interés público a disposición de la ciudadanía. Estas iniciativas están teniendo una gran aceptación y repercusión positiva en la opinión pública, que está demandando una utilización más generalizada de la red.

Una de las más ambiciosa de estas iniciativas, puestas en marcha por la Administración, es el denominado proyecto CERES (CERtificación ESpañola) que lidera la Fábrica Nacional de Moneda y Timbre, y que en líneas generales, consiste en establecer una Entidad Pública de Certificación, que permita autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación.

Las posibilidades de CERES cubren todas aquellas relaciones entre las distintas Administraciones (Central, Autonómica y Local) y los ciudadanos que necesiten ser securizadas en términos de garantía de identidad, confidencialidad e integridad, con el objetivo de que CERES facilite al máximo sus relaciones a través de las nuevas redes de comunicaciones.

El objetivo principal de CERES es la securización de las comunicaciones electrónicas con la Administración, siendo un intermediario transparente al usuario que garantizará a ciudadanos y Administraciones la identidad de ambos partícipes en una comunicación, así como la confidencialidad e integridad del mensaje enviado.

Para ello, CERES utiliza técnicas y sistemas criptográficos basados en lo que se conoce como sistema de clave pública, con dos características básicas:

- La identidad del usuario, al igual que su capacidad de firma, se encuentra, en el caso de máxima seguridad, almacenada en una tarjeta inteligente, que no puede ser accesible salvo por su propietario cuando introduzca el número de identificación personal, similar a la clave de una tarjeta de crédito. En caso de no utilizar tarjeta, el perfil criptográfico queda almacenado en un fichero, siendo necesario también un PIN de acceso.

- El sistema es completamente transparente al usuario, es decir, no es necesario conocer ninguna técnica criptográfica para realizar o verificar una firma electrónica o cifrar o descifrar un mensaje.

2.6.1. Entrevista con Javier Montes Antona

Javier Montes Antona

Dirección de Sistemas de Información

Jefe de Servicio de Relaciones Externas

Departamento CERES

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

Javier Montes Antona: "En certificación electrónica la Fábrica Nacional de Moneda y Timbre pone la seguridad por encima de otros parámetros"

El jefe de servicio de Relaciones Externas del proyecto CERES de la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda apuesta por el servicio público como el principal objetivo de la institución en materia de certificación electrónica.

La Fábrica Nacional de Moneda y Timbre (FNMT) ofrece a los usuarios una confianza tradicional avalada por los distintos productos y servicios que presta la institución desde su creación.

Con el proyecto CERES (CERtificación ESpañola) España da un paso más en el uso de las nuevas tecnologías y apuesta decididamente por Internet como vía de comunicación entre la Administración y la ciudadanía. Liderado por la Fábrica Nacional de Moneda y Timbre (FNMT) el proyecto nace con el objetivo de establecer una entidad pública de certificación que permita autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y las administraciones públicas a través de las redes abiertas de comunicación. El jefe de servicio de Relaciones Externas del proyecto CERES, Javier Montes Antona, defiende esta ambiciosa iniciativa tecnológica promovida por la Administración y destaca, como principal característica, la seguridad y confianza que este servicio ofrece a todos sus usuarios.

"La certificación es un tema de confianza y seguridad", señala Javier Montes, y en este sentido la FNMT ofrece la confianza tradicional avalada por los múltiples y distintos productos y servicios que se ofertan desde hace años - como los pasaportes, los DNI o los sellos – y la confianza adicional de

tener como respaldo al Estado. Además, "FNMT ofrece una seguridad mayor que la que puede ofrecer una empresa privada, que siempre busca los beneficios. No es que nosotros busquemos pérdidas", matiza, "pero ponemos la seguridad por encima de otros parámetros".

Otro valor diferencial que ofrece el servicio prestado por la FNMT con respecto a entidades privadas se basa en la facilidad para la obtención del certificado digital, ya que se dispone de una amplia red de oficinas de registro cercanas a los ciudadanos donde obtener el certificado electrónico Clase 2. Además, este certificado puede obtenerse en el extranjero a través de embajadas y consulados. La obtención del certificado electrónico FNMT Clase 2 es gratuita, y puede solicitarla tanto os españoles como los extranjeros residentes en España que dispongan de un NIE.

La FNMT tiene una parte clave de servicio público, no se pretende rentabilizar cada uno de los productos, sino que se trabaja para tratar de expandir al máximo el uso de la firma electrónica, tanto en la Administración Pública y en las empresas, como en el ámbito nacional e internacional.

Usos del certificado electrónico

Con el certificado electrónico expedido por la FNMT se pueden realizar todo tipo de trámites por Internet de forma que se garantiza la verdadera identidad del usuario, al tiempo que permite firmar electrónicamente formularios y documentos electrónicos con la misma validez jurídica que si se firmara con puño y letra el mismo documento en papel. De este modo el usuario tiene la posibilidad de realizar multitud de gestiones durante las 24 horas del día y evitando desplazamientos y esperas.

El responsable de Relaciones Externas del proyecto CERES destaca que el uso de la certificación electrónica está más extendida en la Administración General del Estado, siendo la Agencia Tributaria líder en este uso para la realización de la Declaración de la Renta. Según detalla, hay más de 100 millones de trámites telemáticos realizados ante la AEAT con este tipo de certificado. El 98 por ciento de las declaraciones de Renta que han sido presentadas a través de Internet han utilizado certificados electrónicos de la FNMT. "Y año a año está creciendo el número de usuarios que utilizan el certificado, y eso es importante". Por otra parte, Javier Montes reconoce que el uso de la certificación electrónica también está ampliamente extendido en otras Administraciones Estatales, como por ejemplo la Seguridad Social, especialmente en lo referido a las consultas sobre vida laboral. "En la Administración Autonómica existen diferentes grados de implantación, aunque estos últimos años hemos asistido a un esfuerzo muy importante por modernizar y agilizar los trámites telemáticos en algunas Comunidades Autónomas, e incluso por parte de algunas Corporaciones Locales. En último lugar hablaría de las empresas privadas, que siguen un ritmo bastante más lento en la adopción de la firma electrónica que las Administraciones Públicas", explica.

Aunque pueda parecer que la certificación electrónica se limita a trámites muy concretos, tal como

detalla Javier Montes Antona, todo proceso nuevo comienza de manera similar y primero se automatizan y modernizan aquellos 4 o 5 trámites que suponen el 80 por ciento de los servicios prestados a los ciudadanos y, posteriormente, se automatizan cientos de ellos que dan lugar al 20 por ciento residual. Así, se comienza con aplicaciones como el padrón, en los ayuntamientos, o el cambio de médico y poco a poco tratamos de optimizar el resto de las prestaciones. "Vamos avanzando, aunque quizás no con la velocidad deseada, sobre todo en estos tiempos de crisis que siempre suponen un freno en estas cosas", asevera.

Consultado sobre el retorno de la inversión realizada en materia de certificación electrónica, el responsable de Relaciones Externas del proyecto CERES reconoce que se trata de un retorno "no inmediato", pero que en esta cuestión el Estado también se mueve por el interés de prestar más y mejores servicios y así se mide el retorno en otros parámetros o valores, como pueden ser la seguridad o los beneficios sociales. "La Administración Pública no mira sólo la rentabilidad inmediata", recuerda Montes Antona, para quien la inversión acabará retornando, "no a corto, sino a largo plazo". En este aspecto, sí considera que la empresa privada se encuentra más limitada porque se mueve a corto plazo y tiene otras opciones distintas a la certificación digital que, aunque no son tan seguras, ofrecen buenos niveles de garantía con costes más asequibles aunque subraya que sí se aprecia que el e-commerce está avanzando mucho con el uso de la factura electrónica.

La FNMT ha emitido ya más de 5 millones de certificados electrónicos, de los cuales 2,5 millones están activos y vigentes. Además, hay cerca de 9 millones de DNIe emitidos. Estas cifras reflejan que hoy en día existe un público todavía minoritario, que ha podido comprobar las ventajas del uso de los certificados electrónicos, como son el evitar desplazamientos, las colas innecesarias y la atención continua.

En este sentido, hay que reconocer la funcionalidad del DNIe, "porque lo llevas siempre encima", si bien se necesita un lector del que no todos los ordenadores disponen y esto supone una barrera que hay que superar, porque no todo el mundo tiene acceso o conocimiento para realizar estas operaciones.

Legislación

En materia de legislación el miembro del proyecto CERES entiende que generalmente las leyes han ido siempre "un poco por detrás de los avances tecnológicos, aunque hoy en día esta cuestión se ha estabilizado". En este aspecto se destacan como puntos clave la Ley 59/2003, del 19 de diciembre, que equipara la firma electrónica con la firma manuscrita, y la Ley 11/2007, del 22 de junio, que obliga a la Administración Pública a dotarse de los medios y sistemas electrónicos que permitan a los ciudadanos a ejercer su derecho a comunicarse con las Administraciones por medios electrónicos. Se define

así una nueva tipología de certificados electrónicos, como son los de sede electrónica, sello para actuación administrativa automatizada y certificado de empleado público.

Cabe destacar aquí el Real Decreto 1671/2009, por el que se desarrolla parcialmente la citada Ley 11/2007 en el ámbito de la Administración General del Estado.

En este sentido, para Javier Montes Antona la actual crisis que vivimos ha supuesto un parón en los avances en esta materia, ya que de darse otra coyuntura económica la Administración Pública hubiera dado un salto "más cuantitativo y cualitativo" en la oferta de servicios a través de Internet. Actualmente se trata de cumplir con la legislación y lo que es importante es tener en cuenta que en este momento cualquier ciudadano puede exigir que cualquier procedimiento esté en Internet.

La Ley 59/2003 equipara la firma electrónica con la manuscrita tanto en el ámbito público como privado. Si bien el uso de certificados electrónicos reconocidos está más extendido en los procedimientos relacionados con la Administración Pública, la percepción de calidad y seguridad de este sistema por parte de los usuarios particulares puede comprometer a las empresas privadas que, con el tiempo, si quieren cuidar su imagen y ofrecer servicios más seguros a través de Internet terminarán por utilizar este tipo de certificados.

Escenario internacional

Consultado sobre el uso de la certificación electrónica a nivel internacional, el responsable de Relaciones Externas del Proyecto CERES explica que hay proyectos a nivel europeo y global pero que se están chocando con diversas dificultades, sobre todo de interoperabilidad, porque hay diferentes sistemas de uso de los certificados, como las certificaciones cruzadas, en las que es difícil delimitar las responsabilidades entre las partes. "A fecha de hoy en día todavía no se ha llegado a una solución global", concluye.

Asimismo, Javier Montes Antona explica que en julio de este año la Comisión Europea adjudicó a la FNMT un contrato de servicios PKI (Infraestructura de Clave Pública). Esto significa que la FNMT es el Proveedor de Servicios de Certificación que emitirá los certificados electrónicos de los empleados de la Comisión Europea y de 27 Instituciones y Agencias de la Unión Europea, así como los certificados de los servidores web de éstas.

Comunidades Autónomas ante la certificación

Las Comunidades Autónomas de País Vasco, Cataluña y Valencia se han convertido en entidades de certificación o prestadores de este tipo de servicios. Para Montes Antona el hecho de convertirse en

entidad de certificación no se trata de una cuestión de ahorro económico, puesto que es más rentable compartir recursos que desarrollar un servicio propio; ni de compatibilidad o tecnológico, sino que se trata más bien de una manera de tratar de defender la propia identidad autonómica a través de una certificación propia.

"Para mi la identidad se manifiesta mejor mediante la inversión en la mejora de los propios servicios que prestas a tus ciudadanos telemáticamente", apunta Montes Antona, quien personalmente cree en una inversión "más orientada a los servicios que ofrezcan más valor y pensando que hay un camino largo de cara a ofrecer el 100 por cien de los servicios al ciudadano de manera telemática".

En este punto, considera que las comunidades autónomas han avanzado de manera notable en materia de adaptación a la Ley 11/2007. "Estamos bastante avanzados, aunque sería difícil cumplirla en su totalidad, pero llevamos un buen camino", subrayó.

Visión de futuro

El futuro de la certificación electrónica pasa, para el responsable de Relaciones Externas del Proyecto CERES, en la capacidad para mirar hacia Europa e interoperar con la Unión Europea en un primer nivel y con el resto de los países en otro segundo nivel, llevando a cabo macroacuerdos entre las entidades.

Sobre la pervivencia de los proveedores de servicios de certificación será la ley de la oferta y la demanda la que decida cuáles continuarán y cuáles desaparecerán, cuyos certificados tendrá que asumir por obligación el Ministerio de Industria. "Posiblemente los pequeños proveedores desaparecerán o deberán hacer alianzas. El propio mercado es el que dirá", apostilla Montes Antona.

2.7. INTECO, Instituto Nacional de Tecnologías de la Comunicación

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) es una sociedad mercantil estatal, con sede en León (España), adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Está participada al 100% por la Entidad Pública Empresarial red.es.

INTECO se crea, previa autorización del Consejo de Ministros en su reunión de 27 de enero de 2006, para responder a un doble objetivo: por un lado, contribuir a la convergencia de España con Europa en el ámbito de la Sociedad de la Información desarrollando proyectos innovadores en el ámbito de la tecnología de la comunicación y, por otro, promover el desarrollo regional, enraizando en León un proyecto con vocación global.

INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas Tecnologías de la Información y la Comunicación (TIC) en España, en clara sintonía con Europa.

Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

Por otra parte, INTECO aparece expresamente constituida como medio propio y servicio técnico de la Administración General del Estado, con lo que está obligada a realizar los trabajos que le encomienden los diferentes departamentos ministeriales de la Administración General del Estado en las materias objeto de sus funciones de una forma ágil y eficaz a través de la figura de las encomiendas de gestión.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en España, promoviendo además una línea de participación internacional.

La visión de INTECO es conseguir sus objetivos mediante:

- El compromiso de profesionales altamente cualificados, comprometidos con sus proyectos y capaces de generar valor e innovación continuamente.

- La dinamización del sector TIC, generando nuevos negocios y oportunidades para clientes, proveedores y profesionales.

- La igualdad de oportunidades para todo el tejido empresarial español, especialmente la pyme, actuando como suministro de último recurso en materia de innovación TIC allá donde sea necesario.

- El soporte a los ciudadanos, que son la clave para que el desarrollo de las nuevas tecnologías tenga un impacto social positivo.

2.7.1. Entrevista con Marcos Gómez Hidalgo

Marcos Gómez Hidalgo

Subdirector Programas

Direccion de Operaciones

INTECO: Instituto Nacional de Tecnologias de la Comunicacion

INTECO apuesta por la formación y la sensibilización como claves para acercar las aplicaciones de la certificación digital, entre ellas la firma electrónica, a la ciudadanía

El subdirector de Programas del Instituto Nacional de Tecnologías de la Comunicación, Marcos Gómez Hidalgo, subraya que es en la Administración Pública y las empresas donde está más extendido el uso de esta nueva tecnología.

Para Gómez Hidalgo es necesario que los usuarios conozcan que al implementar/utilizar servicios con certificados digitales (en particular con firma digital) se producen ahorros de costes y tiempo y de eficiencia frente a los mismos servicios sin esta tecnología.

Divulgar el uso y las ventajas de las aplicaciones de los certificados digitales, principalmente la firma electrónica, entre la ciudadanía y superar las dificultades, tanto técnicas como de formación, en esta materia son los retos que se plantea el Instituto Nacional de Tecnologías de la Comunicación (INTECO) de cara al futuro. Hoy en día la complejidad técnica, el desconocimiento general de su utilidad y la falta de confianza en esta nueva tecnología son las principales dificultades con las que el ciudadano de a pie se encuentra a la hora de introducirse en el uso de la firma electrónica. Así lo explica el subdirector de Programas de INTECO, Marcos Gómez Hidalgo, quien plantea como objetivo superar estas barreras, difundir entre la ciudadanía las ventajas que los certificados digitales pueden ofrecerles, tanto en ahorro de costes como de tiempo, y al mismo tiempo favorecer el desarrollo de nuevos servicios, públicos y privados, en los que se pueda operar con confianza, con certificados digitales.

Bajo el nombre de INTECO funciona desde 2006 una entidad de carácter público, dependiente del Ministerio de Industria, Turismo y Comercio, que tiene un doble objetivo: contribuir a la convergencia de España con Europa en el campo de la sociedad de la información a través de proyectos innovadores en tecnología de la comunicación; y, por otra parte, promover el desarrollo regional. Así, el centro sirve de instrumento para desarrollar la sociedad de la información en España, en sintonía con Europa, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres puntos clave: la investigación aplicada, la prestación de servicios y la formación.

Desde su creación INTECO trabaja en ámbitos estrechamente relacionados con la firma electrónica, tanto en lo referente a concienciación y sensibilización, como con el apoyo a desarrolladores o el soporte a usuarios y pymes. La difusión del DNIe es uno de los campos básicos de actuación de la entidad, que también ofrece servicios de consultoría en clientes a la Administración Pública.

Uso de los certificados digitales

En la actualidad el uso de la certificación digital está más extendido en el ámbito de la Administración Pública, encargada también de impulsar estas nuevas tecnologías, mientras que en la empresa se emplea principalmente para facturación electrónica o en iniciativas concretas de ciertos sectores, como la banca. Facturación electrónica y contratación electrónica son los sectores donde la certificación digital tiene mayor promoción. Por el contrario, la ciudadanía sigue descolgada del tren digital y, aunque los trámites con la Agencia Tributaria y el DNIe son los usos más difundidos, distan aún mucho de los niveles deseados. Por esto, el responsable de Programas de INTECO considera fundamental difundir las ventajas del uso de los certificados digitales entre las empresas, ciudadanos y Administraciones Públicas. Con la administración electrónica se optimizan costes y tiempo, se simplifican los procesos y se atiende al ciudadano de una manera más eficiente y segura, tal como explica Marcos Gómez Hidalgo. Por su parte, el ciudadano obtiene como principal beneficio una flexibilidad de horarios y ubicuidad, al tiempo que ve reforzada su confianza en el prestador del servicio.

Sobre la percepción de seguridad que ofrece la firma digital para el ciudadano, el subdirector de Programas de INTECO considera que los usuarios critican más las dificultades técnicas a la hora de aplicar los certificados digitales que la seguridad de los mecanismos de la firma. Además muchos usuarios demandan una separación entre el uso particular y el uso profesional de los certificados digitales. Gómez Hidalgo subraya la necesidad de atajar esta situación de desconocimiento sobre la firma digital a través de iniciativas de formación, concienciación y sensibilización.

Legislación

La legislación española actual es "suficiente, clara y completa" en materia de regulación de certificación digital y firma electrónica ya que, además la normativa propia, se traspone la directiva europea en cuanto a tipología, características y tipos de uso. En esta línea Marcos Gómez Hidalgo destaca que España es, con el DNIe "una potencia de primer orden en certificados digitales", una situación de liderazgo que es reconocido en Europa.

Consultado sobre la compatibilidad legislativa de la certificación digital en los diferentes países, el subdirector de Programas de INTECO explica que a nivel europeo la propia Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, establece ya un marco comunitario para la firma electrónica. Esta normativa propicia un marco legislativo común en los países europeos, mientras que a nivel internacional todavía "queda un largo camino por recorrer en cuanto a interoperabilidad", al tiempo que las diferencias terminológicas pueden dar lugar a confusiones entre individuos procedentes de distintos países o en contratos internacionales.

Autonomías y certificación digital

En relación al papel que juegan las Comunidades Autónomas como prestadoras de servicios de certificación digital, Marcos Gómez Hidalgo considera que este tipo de proyectos ofrecen el valor añadido de independencia a las propias comunidades, al tiempo que ponen a disposición del usuario servicios que permiten un aumento de confianza con mayor eficiencia y trámites más simplificados. Por el contrario, estas iniciativas propias pueden repercutir en el precio de los servicios prestados, ya que requieren una inversión por parte de las Comunidades Autónomas, y eventualmente se pueden ocasionar retrasos si fuera necesario contactar con otra entidad para comprobar la validez de certificados externos.

Aunque, tal como señala Gómez Hidalgo, resulta difícil medir el retorno de las inversiones que las Comunidades Autónomas realizan en estos proyectos propios, debe valorarse que las iniciativas autonómicas, además erigirse en referentes para las empresas, pueden aprovecharse para consolidar la posición de España en materia de certificación digital, en particular con el uso del DNIe, pionero en su campo.

Futuro del certificado digital

El futuro presenta grandes retos a superar en el campo de la certificación digital. Además de los avances propiamente tecnológicos y la difusión a nivel usuario, se plantea cómo convivirán a largo plazo las entidades de certificación públicas y privadas. En este aspecto, el subdirector de Programas

de INTECO lo tiene claro: "cumpliendo la legislación pueden convivir ambos tipos de entidades, cada una tendrá su ámbito de aplicación", ya que la propia normativa establece obligaciones y responsabilidades de los prestadores de servicios de certificación y los requisitos para su acreditación como tales. Además de este hecho, considera clave la especialización de cada entidad en un campo concreto, así como la generación de servicios de valor añadido y la adaptación de producto/servicio y coste. Para Gómez Hidalgo incluso es necesaria la coexistencia de redes de autoridades nacionales o sectoriales, interrelacionadas entre sí y con servicios propios a usuarios de sus respectivos ámbitos de actuación.

Por otra parte, Marcos Gómez Hidalgo aborda también los principales retos de la firma electrónica tanto en España como en Europa a largo plazo. En este sentido considera que un aspecto fundamental es trabajar en la difusión y formación de esta tecnología a todos los niveles: usuarios, empresas, desarrolladores y administraciones, a lo que deberá unirse una regulación legislativa adecuada y común a toda el área de aplicación.

Además, Gómez Hidalgo considera necesario avanzar en la creación de Autoridades de Certificación Pública gratuitas que ofrezcan los servicios básicos de emisión de certificados personales, de empresa y de facturación, validación y sellado de tiempo, entre otros, asociados a los correspondientes servicios de mantenimiento; y en la conformación de un estándar que regule el uso de la firma electrónica en la Administración Pública, abordando cuestiones como la funcionalidad, aspectos visuales identificativos o tratamiento de documentos firmados. La puesta en marcha de estos proyectos de futuro supondría, según Gómez Hidalgo, una serie de oportunidades de negocio interesantes a determinar.

Y ante los retos de futuro de la certificación digital el Instituto Nacional de Tecnologías de la Comunicación no puede quedar indiferente. Así, entre sus principales apuestas a largo plazo INTECO se marca como meta avanzar en materia de concienciación y sensibilización a través de programas formativos; colaborar con la Administración Pública en proyectos de firma electrónica; apoyar el desarrollo y la certificación de aplicaciones de firma con DNIe; y dar soporte a la liberalización de aplicaciones de software de validación y firma electrónica, entre otras cuestiones. En general, el organismo público trabajará en todas aquellas propuestas que contribuyan a generar confianza en el uso de los servicios de la sociedad de la información, una clara apuesta por las nuevas tecnologías al servicio de la sociedad.

2.8. IZENPE, ZIURTAPEN ETA ZERBITZU ENPRESA

Izenpe S.A., Ziurtapen eta Zerbitzu Enpresa/Empresa de Certificación y Servicios, es una sociedad anónima constituida en 2002 y supone un proyecto impulsado por el Gobierno Vasco y las Diputaciones Forales constituido a través de sus diferentes sociedades informáticas:

- EJIE (Eusko Jaurlaritzaren Informatika Elkartea/Sociedad Informática del Gobierno vasco): es una empresa pública del Gobierno Vasco que contribuye, mediante la prestación de servicios informáticos, a conseguir una Administración Pública Vasca moderna y eficiente.

- LANTIK S.A.: es una sociedad de carácter unipersonal, participada exclusivamente por la Diputación Foral de Bizkaia, que fue constituida en el año 1981 con la finalidad de proveer a la Institución foral, a los organismos e instituciones que dependen de la misma y a los ayuntamientos de Bizkaia de sistemas de información, encargándose, igualmente, de la explotación de los mismos y de la prestación de todo tipo de servicios anexos.

- IZFE S.A. (Informatika Zerbitzuen Foru Elkartea/Sociedad Foral de Servicios Informáticos): tiene por objeto la prestación de servicios informáticos que garanticen la consecución de la línea estratégica de los sistemas de información de la Diputación Foral de Gipuzkoa en el entorno de las tecnologías de la información y las comunicaciones

- CCASA S.A.: tiene por objeto prestar los servicios que garanticen la consecución de la visión estratégica de los sistemas de información de la Diputación Foral de Álava en el entorno de las tecnologías de la información y comunicaciones.

Los objetivos generales de Izenpe son los siguientes:

- El fomento del uso y potenciación del desarrollo del gobierno electrónico sobre redes de telecomunicaciones con las necesarias garantías de seguridad, confidencialidad, autenticidad e irrevocabilidad de las transacciones.

- La prestación, en el ámbito de las instituciones que integran el sector público vasco, de servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos.

- La expedición, fabricación y suministro de los títulos o certificados de usuario o soportes en tarjeta necesarios para personas o entidades públicas o privadas.

- La expedición, fabricación y suministro de los títulos o certificados de servidor.
- Servicios de Consultoría relacionados con la promoción del gobierno electrónico.

2.8.1. Entrevista con Eduardo Portero Delgado

Eduardo Portero Delgado

Director General

Izenpe S.A., Ziurtapen eta Zerbitzu Enpresa/Empresa de Certificación y Servicios

Eduardo Portero Delgado: "Las funciones de Izenpe van mucho más allá de ser un simple prestador de servicios de certificación digital, ahora nuestro objetivo es definir procesos de administración electrónica"

Para el director general de Izenpe hoy en día una Comunidad Autónoma no es sólo un tercero de confianza como emisor de certificados digitales, sino que puede ofrecer nuevos servicios y situarse a la vanguardia de la e-administración.

Izenpe es uno de los dos únicos proveedores mundiales de certificados de servidor seguro SSL con SV, un documento con gran aplicación y demanda en la actualidad.

En un marco nacional en el que en los últimos años han nacido nuevas necesidades en materia tecnológica la certificación digital se convierte en un mercado en desarrollo. A la creación de organismos a nivel estatal, públicos y privados, prestadores de servicios de certificación digital se han unido también las iniciativas de las comunidades autónomas, dispuestas a no perder el tren del progreso tecnológico y a disponer de autoridades propias, diferentes y adaptadas a su realidad. En este marco se constituye en el año 2002 Ziurtapen eta Zerbitzu Enpresa – Empresa de certificación y servicios Izenpe S.A., una sociedad anónima impulsada por el Gobierno Vasco y las Diputaciones Forales. Su director general, Eduardo Portero Delgado, explica los motivos de su creación como una decisión política, "porque tener un prestador de servicios de certificación digital es caro si se quiere que sea realmente operativo". Pero afirma que, ocho años después de su puesta en marcha, las funciones de Izenpe "van mucho más allá de ser un simple prestador de servicios de certificación digital". "Todo lo relacionado con la emisión de certificados funciona bien y de manera automática", explica, "ahora el objetivo es la definición de procesos de administración electrónica".

Para Eduardo Portero Delgado la creación de autoridades de certificación digital propias en las comunidades autónomas está justificado porque éstas pueden cumplir otra serie de cualidades. "Hoy en

día una Comunidad Autónoma no es sólo un tercero de confianza o un mero validador que da crédito y fe, sino que puede ofrecer una cantidad de servicios, al tiempo que debe ser la vanguardia de la administración electrónica", apunta. En este sentido, destaca que en la actualidad Izenpe se encuentra a la vanguardia en el desarrollo de servicios de consultoría y de estudios para la Dirección de Innovación y Administración Electrónica del Gobierno Vasco.

Productos y servicios

Según explica el director general de Izenpe, la mayor parte de sus clientes se sitúa en el sector público, ayuntamientos, diputaciones y el Gobierno Vasco; mientras que los clientes de la empresa privada demandan productos tecnológicos y trabajos de consultoría. En este punto, Portero Delgado destaca el hecho de que en certificación digital Izenpe es una de las dos únicas entidades en todo el mundo que proporcionan certificados de servidor seguro SSL con SV, un certificado con gran aplicación debido a la demanda cada vez mayor de seguridad en los entornos de Internet.

En general, los objetivos de Izenpe pasan por fomentar el uso y el desarrollo del gobierno electrónico sobre redes de telecomunicaciones con las necesarias garantías de seguridad, confidencialidad, autenticidad e irrevocabilidad de las transacciones. Así, trabaja en la prestación, en el ámbito de las instituciones que integran el sector público vasco, de servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos. Los principales documentos que emite son certificados digitales de usuario o soportes en tarjeta para ciudadanos y para entidades, públicas o privadas; así como certificados corporativos, que son certificados privados para las personas de una empresa. Izenpe también presta servicios de consultoría relacionados con la promoción del gobierno electrónico. Además, según señala el director general de la entidad, en su estrategia se incluye seguir ampliando el número de certificados en función de los proyectos de administración electrónica que surjan y en función de la propia demanda.

En lo referente a productos, el más demandado es la plataforma de servicios de firma integrados ZAIN, tal como apunta Portero Delgado. Además, Izenpe ofrece otros productos como son el servicio de constancia de la publicación para la firma electrónica; y el Lotura@, un broker de identidades o agente mediador, que funciona de tal manera que dos entidades que "compren" el producto disponen de un tercero de confianza (Izenpe), lo que les permite intercambiar determinados datos. Actualmente este sistema se utiliza en la Diputación foral de Gipuzkoa para conectar las aplicaciones de tráfico de las policías locales con el Ministerio del Interior.

En este punto, el responsable de Izenpe destaca que el proyecto más importante de Izenpe es la tarjeta ONA, que ha supuesto la principal línea de negocio del organismo. Según los datos que maneja, actualmente hay aproximadamente 250.000 tarjetas ONA emitidas, un documento que funciona

como "una tarjeta sanitaria para usos ciudadanos". La ONA tiene asociados dos tipos de servicios: electrónicos y eléctricos. El uso fundamental de esta tarjeta es el sanitario y sólo un porcentaje mínimo de ciudadanos ha utilizado esta tarjeta para realizar trámites telemáticos. "El grado de usabilidad de la tarjeta ONA, cuyo coste ha sido muy elevado, es todavía muy bajo –en torno al 3 por ciento-, pero con un grado de satisfacción muy alto", lamenta Eduardo Portero Delgado. Esto se debe, según apunta, a que muchos ayuntamientos no tienen realizados los desarrollos necesarios para realizar trámites electrónicamente, lo que limita el uso de los dispositivos. Y el futuro se presenta difícil para esta tarjeta, ya que el Parlamento Vasco ha aprobado una proposición no de ley en la que pone fin a dicho proyecto el próximo 31 de diciembre, lo que significa que Izenpe no emitirá más tarjetas ONA, aunque sí está obligado a custodiar la documentación durante 15 años, a mantener el certificado electrónico vivo durante 4 años y a operar con los servicios asociados al plástico durante 10 años.

Convergencia de dispositivos

El futuro de la certificación digital pasa por unificar dispositivos y definir usos y funciones. Así lo expone el director general de Izenpe, quien considera que si realmente se quiere convertir al ciudadano en un ciudadano digital es necesario realizar una convergencia de dispositivos, es decir, unificar todos los dispositivos electrónicos en uno sólo, manejable y comprensible. "Que los ciudadanos vean que la e-administración es una realidad, que es ventajosa y que les va a proporcionar mejores relaciones con la administración dependen de que haya una tendencia real a la unificación de los dispositivos electrónicos", plantea Portero Delgado.

A juicio de Eduardo Portero Delgado es necesario replantearse para qué vale la firma electrónica y en qué ámbitos tiene sentido su utilización, para lo que la Administración Pública debe hacer esfuerzos en el despliegue de aplicaciones y desarrollo de tarjetas como instrumentos para el uso de estas aplicaciones. "Hasta ahora se ponía por delante el despliegue de tarjetas antes que el desarrollo de los sistemas de información que las iban a utilizar", apunta, una situación que debe cambiar.

Además, en este punto, Portero Delgado hace referencia a los nuevos usos de futuro que ofrece la biometría, cuyo uso complementario se asocia hoy en día a la firma electrónica para aquellos entornos "muy delicados".

Normativa vasca

El director general de Izenpe se refiere también a la normativa legal en la que se enmarca la certificación digital. En este sentido, recuerda que el Gobierno Vasco dispone del Decreto de uso de medios electrónicos, informáticos y telemáticos en los procedimientos del Gobierno Vasco, una normativa propia de la Comunidad Autónoma en cuanto a la admisión de medios telemáticos en la que se es-

tablecen los escenarios y condiciones técnicas que deben tener los prestadores de certificación para que sus documentos sean válidos en el ámbito de la comunidad. De esta forma, cualquier autoridad de certificación digital que desee operar en el País Vasco debe homologarse según los requisitos establecidos en este decreto.

Sobre este decreto, Eduardo Portero Delgado reconoce que aunque el decreto "es el envoltorio que ha permitido a Izenpe doblegar al resto de prestadores de servicios de certificación digital para admitirlos o no, la tendencia es que en un futuro inmediato haya la obligación a que todos los prestadores en el marco europeo se admitan entre ellos". Así, apunta a que se tenderá "hacia la conjunción de sistemas tecnológicos e informáticos" y se muestra convencido de que "habrá un marco europeo de homologación único". En concreto, Portero Delgado explica que actualmente se está discutiendo sobre cómo liberar las políticas en materia de certificación digital (de hecho, la Unión Europea trabaja ya en la definición de las políticas de certificados en todo su territorio) ya que, todavía ahora, existen certificados con políticas muy restrictivas, lo que provoca que en algunos casos una persona disponga de varios certificados. A su juicio, esta situación también determina la necesidad, antes apuntada, de que funcione un organismo de carácter supranacional que realice las validaciones de identidad.

Legislación general

Más allá de la normativa propia vasca en materia de certificación digital, el máximo responsable de Izenpe aborda también la situación legal a nivel estatal. Al tiempo que reconoce que gran parte del despliegue de la administración electrónica se ha hecho "a golpe de ley", para él la Ley 11/2007, del 22 de junio, es "buena, porque es flexible", aunque a su juicio peca de incluir el condicionante de la disponibilidad presupuestaria, algo que limita su desarrollo y aplicación práctica.

"La ley ya es suficientemente amplia, no son necesarias nuevas coberturas legales, lo necesario es la voluntad amplia, clara y concisa por parte de la Administración Pública", explica Portero Delgado, quien detalla que esta voluntad debe basarse en explicar claramente al ciudadano qué es lo que puede hacer de una manera sencilla y clara. Además, incide en la importancia de elaborar aplicaciones que garanticen que cualquier usuario podrá operar utilizando el entorno que desee, es decir, que se garantice el principio de interoperabilidad y de neutralidad tecnológica.

En este punto Portero Delgado insiste de nuevo en la necesidad de caminar hacia una normativa común ya que considera que un exceso de leyes y reglamentaciones propias de administración electrónica –a nivel de ayuntamientos, comunidades autónomas, etc...- puede provocar inseguridad jurídica. "Hay que evitar el deseo de originalidad de las Administraciones Públicas en cuanto a la legislación en torno a la e-administración", concluye.

A modo de apunte, Eduardo Portero Delgado destaca que Avilés es el ayuntamiento de España con

mayor desarrollo de la administración electrónica, pero que la mayor parte de los trámites se realizan simplemente con nombre de usuario y password, lo que ofrece un bajo grado de seguridad.

Usos de la certificación digital

"Los ciudadanos que utilizan la firma electrónica es porque tienen claro su valor de seguridad", apunta tajante el director general de Izenpe, "otra cosa es que lo vean como algo eficaz", añade. Para Eduardo Portero Delgado la ciudadanía en general tiene claro que la firma electrónica es un sistema seguro, pero todavía no han visto ni su utilidad ni su eficacia. De hecho, según detalla, varios estudios apuntan a que la satisfacción de los ciudadanos ante el uso de tarjetas inteligentes estaría relacionada con el incluir en las mismas medios de pago y medios para el acceso al transporte público. En todo caso, para Portero Delgado esto es un ejemplo de la demanda que existe entre la población para disponer de una sola tarjeta con todos los usos posibles: lo que se conoce como convergencia digital.

En el caso concreto del País Vasco, donde las diputaciones son las encargadas de recaudar los tributos, el principal uso de la firma electrónica se registra en la facturación electrónica. Para ello Izenpe desarrolló un producto a instancia de las propias diputaciones, que veían la necesidad de disponer de un sistema de facturación electrónica. Además, el mismo organismo público de certificación digital trabaja de manera habitual con factura electrónica e intenta que todos sus proveedores facturen a través de este sistema.

Retos de futuro

Consultado sobre la convivencia futura de las entidades de certificación públicas y privadas el responsable de Izenpe resuelve: "Todos los prestadores de servicios de certificación comparten un espacio común, y la competencia y la competitividad son buenas". Ademas, añade, "la colaboración actual de Izenpe es muy buena con todos los prestadores de servicios existentes y así debe ser, debido a la importancia de todos los temas relacionados con el entorno de la certificación".

En esta línea, para Eduardo Portero Delgado lo más lógico será que en un escenario próximo exista una política común de identificación de los nacionales, es decir, que Europa cree una autoridad común en materia de identificación digital. A su parecer, al igual que pueden nombrarse cinco aspectos comunes que identifican físicamente a todos los ciudadanos europeos, se deberá definir una serie de aspectos que los definen electrónicamente, lo que llevará a crear un sistema común de identificación.

Sobre el futuro de la firma electrónica, para Portero Delgado el éxito del desarrollo y del uso de este tipo de certificado digital vendrá marcado por la existencia de un validador a nivel supra-nacional,

junto con la implementación de elementos biométricos asociados y complementados a la firma digital para entornos delicados. Además, se muestra convencido de que serán el propio mercado y los usuarios los que marcarán tendencia en todas las soluciones y retos futuros en este campo. Así, pone como ejemplo el hecho de que en la actualidad "hay usuarios y entornos que piden cada vez más seguridad en la red, por lo que es necesario dar un determinado grado de fiabilidad", lo que obliga a empresas e instituciones a trabajar en esta área. Así, demandas como esta se trasladarán a todos los campos de uso y desarrollo de las nuevas tecnologías.

2.9. Secretaría Xeral de Modernización e Innovación Tecnolóxica de la Xunta de Galicia

La Secretaría Xeral de Modernización e Innovación Tecnolóxica se configura como el órgano superior de la Administración autonómica al que le corresponde el impulso, asesoramiento técnico y apoyo en materia de tecnologías de la información y las comunicaciones y su aplicación para la modernización, innovación y desarrollo tecnológico de Galicia.

Este departamento depende directamente del presidente de la Xunta y nace con vocación de apoyar y dar servicio a las diferentes consejerías, buscando la calidad, racionalización de las actuaciones y la mejora de la eficiencia en la gestión de las TIC.

Su creación supone la constatación de que las tecnologías de la información y las comunicaciones (TIC) constituyen un instrumento de alto nivel estratégico por su potencial para impulsar la modernización de la Administración pública, así como su capacidad para impulsar y sustentar el desarrollo social y económico de Galicia.

Para la consecución de sus objetivos, que no son otros que los expuestos en el programa y el discurso de investidura del presidente, es imprescindible la colaboración de todos los departamentos y organismos de la Xunta.

La Secretaría Xeral de Modernización e Innovación Tecnolóxica debe asumir la evolución permanente de las TIC de la Xunta para mejorar la eficiencia y acercar la Administración al ciudadano y liderar la incorporación plena de la sociedad gallega al mundo de las TIC.

Esto se traduce en los siguientes objetivos:

- Promover un avance significativo de Galicia en el marco de la sociedad de la información.

- Ordenar y homogeneizar las actuaciones en materia de TIC de toda la administración gallega (todos avanzando en la misma dirección), garantizando la seguridad de la información y la interoperabilidad de los sistemas.

- Extraer el máximo aprovechamiento de las posibilidades de las TIC como dinamizador económico, elemento clave de desarrollo sostenible y generador de ahorros.

- Adaptar la Administración gallega a las demandas sociales y los requerimientos legales (Ley de acceso electrónico de los ciudadanos a los servicios públicos) en cuanto a la Administración Electrónica.

2.9.1. Entrevista con Mar Pereira Álvarez

Mar Pereira Álvarez

Secretaria Xeral de Modernización e Innovación Tecnolóxica

Presidencia

Xunta de Galicia

Mar Pereira: "La implantación de la firma electrónica nos permitirá avanzar hacia una Galicia 2.0"

La Secretaria Xeral de Modernización e Innovación Tecnolóxica de la Xunta de Galicia apuesta por abordar de manera integral la acreditación digital de todas las personas que intervienen en el proceso electrónico.

"El crecimiento experimentado por el DNI electrónico en Galicia en el último año fue de un 47,7%".

Para la Secretaria Xeral de Modernización e Innovación Tecnolóxica de la Xunta de Galicia, Mar Pereira, en la medida en que la relación de los ciudadanos y la administración avanza hacia el contexto digital es imprescindible asegurar que este tránsito se hace generando un entorno de confianza en la aplicación de las tecnologías. Ya la propia Ley 11/2007 establece que "el tránsito del procedimiento en papel al empleo de las nuevas tecnologías no favorezca un menoscabo de las garantías".

"El desarrollo de la administración electrónica en la administración pública de Galicia exige abordar de manera integral la acreditación digital de todos los intervinientes en el proceso electrónico", asegura Mar Pereira. Por eso uno de los ejes de actuación del plan de modernización es facilitar a todos sus trabajadores de los medios que les acrediten digitalmente y les habiliten con las capacidades de firma electrónica necesarias para el desempeño de sus funciones.

En este sentido están en marcha una serie de medidas, entre las que cabe destacar, la adjudicación del servicio de certificación digital a la Fabrica Nacional de Moneda y Timbre y el proyecto de acreditación digital del empleado público.

"El recientemente publicado decreto de administración electrónica de la Xunta de Galicia, Decreto 198/2010, do 2 de diciembre, por el que se regula el desarrollo de la Administración electrónica en la Xunta de Galicia y en las entidades de ella dependientes, prevé el marco general de aplicación de esta acreditación y la elaboración de las normas técnicas para su desarrollo", recuerda la secretaria xeral.

En este mismo ámbito se plantea además la necesidad de avanzar a un mayor nivel de uso del DNIe, como instrumento de acreditación digital del ciudadano, por lo que los servicios que se ofrecen por parte de las administraciones deben estar adaptados a su utilización.

Por otra parte, el desarrollo de la eAdministración en el ámbito de los ayuntamientos es un eje fundamental para la prestación de los servicios públicos en iguales condiciones de calidad a todos los ciudadanos y empresas independientemente de su lugar de residencia. En este sentido y para facilitar este desarrollo a las administraciones locales, y a otras entidades, el contrato firmado con la FNMT prevé la adhesión al consumo de estos servicios de la administración local y otros entes de la comunidad autónoma sin coste para ellas.

Este proceso deberá ir acompañado de una formación específica de los conocimientos que permitan a los empleados públicos de la Administración gallega el máximo aprovechamiento de los medios puestos a su disposición.

"No cabe duda que en los últimos años se ha producido un avance considerable en la extensión del uso de la certificación digital ya no sólo gracias a la oferta de servicios públicos por parte de las Administraciones Públicas sino también gracias a la progresiva disponibilidad del DNIe por parte de los ciudadanos".

"Atendiendo a estos dos factores creemos que, en este momento, son las Administraciones Públicas las que permiten un uso más extendido de la certificación digital. Galicia presenta buenos resultados en el uso de los servicios de la eAdministración por parte de la ciudadanía. En el año 2010, el 51,7% de la población gallega que utilizó Internet obtuvo información de páginas web de la administración, superando a la media estatal en 5,3 puntos porcentuales. Un 20,3% envió formularios cumplimentados a través de Internet (2,6 puntos por encima de la media estatal)", asegura Mar Pereira.

Estos datos sitúan a Galicia como la tercera comunidad autónoma con mayor uso de la Administración electrónica para obtener información de las páginas web y la quinta comunidad en descarga y cumplimentación de formularios oficiales.

Además, un 35% de los ciudadanos de Galicia, entre 16 y 74 años, ya disponen del DNI electrónico, 7,5 puntos más que la media estatal, y un 8% dispone de otros certificados de firma reconocidos. El crecimiento experimentado por el DNI electrónico en Galicia en el último año fue de un 47,7%.

"Estos datos indican que tenemos una buena base para afrontar los cambios y los futuros retos de la Sociedad de la Información. Desde el Gobierno gallego y las distintas administraciones debemos impulsar el uso y aprovechamiento de las TIC y fomentar que el ciudadano desarrolle una cultura digital y adquiera seguridad y confianza en su uso", afirma la titula de la Secretaría Xeral de Modernización e Innovación Tecnolóxica.

Es una de las líneas de trabajo de la Axenda Dixital 2014.gal, la estrategia tecnológica global de la Xunta, que contempla el aprendizaje en el ámbito tecnológico como un proceso permanente. Por eso, entre otras medidas, se pondrá en marcha este año, la Red CeMIT de aulas de acceso público a las nuevas tecnologías que tutorizará a la ciudadanía con mayores dificultades para poder integrar las TIC en su vida cotidiana. Además, la Red promoverá la formación digital entre los profesionales gallegos y mostrará a las PYMES y micropymes las ventajas de la sociedad da información. Desde estas aulas se difundirán los servicios de la Administración electrónica y se capacitará a los ciudadanos para emplearlos.

e-Administración y Legislación

Desde el punto de vista de la secretaria xeral, la Ley 11/2007 se encamina a implantar decididamente la Administración electrónica superando las disposiciones de carácter meramente facultativo contenidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Siguiendo esta línea, recientemente, ha sido publicado en el DOG el Decreto 198/2010 que establece el marco de desarrollo de la Administración electrónica en la Administración pública gallega. Así, el objetivo del Gobierno gallego es avanzar en la mejora de la calidad y de la eficacia de los servicios ofrecidos y en el impulso de la eAdministración para una mayor eficiencia interna y en las relaciones intra e interadministrativas. Se trata de conseguir una Administración más transparente y abierta a los ciudadanos las 24 horas los 365 días del año.

El cumplimiento de este objetivo supone para la Administración un gran reto, al exigirle disponer en un corto plazo (2013), de nuevos medios de comunicación y de herramientas tecnológicas que se integren con los sistemas de información existentes y permitan su evolución futura, independientemente de su implantación anterior paulatina.

Por tanto, la Administración gallega ofrecerá a los ciudadanos la posibilidad de realizar las gestiones de manera telemática, con evidentes ventajas para los usuarios: se evitan desplazamientos, los trámites se pueden realizar en cualquier momento y las gestiones se llevan a cabo de manera sencilla. Además, supone un importante paso en materia de reutilización de la información pública en nuestro país.

Así, la Xunta de Galicia por medio del protocolo de interoperabilidad se publicará este año, establecerá los criterios y recomendaciones que deberán ser tenidos en cuenta para la toma de decisiones tecnológicas que garanticen la interoperabilidad y que eviten la discriminación a los ciudadanos por razón de su elección tecnológica. Además, debemos crear las condiciones necesarias para asegurar un adecuado nivel de interoperabilidad que permita el ejercicio de derechos y el cumplimiento de

deberes a través del acceso electrónico a los servicios públicos.

"Queremos que con el trabajo de todos logremos una Galicia 2.0.", resume de manera gráfica Mar Pereira.

El futuro

Desde el punto de vista de la entrevistada, el principal reto de España y Europa en los próximos años en cuanto a la Administración Electrónica en términos generales es sacar el máximo partido de las TIC para evolucionar la Administración Pública a parámetros más altos de inteligencia, sostenibilidad e innovación, y por consiguiente maximizar su potencial económico y social. "La certificación digital y la firma electrónica son elemento muy importantes en este reto porque en muchos servicios en línea resulta esencial identificar y autenticar a la persona física o jurídica a la que se van a prestar."

"Su plena expansión deberá vencer las posibles barreras que suponga la desconfianza por parte del ciudadano", asegura Pereira. La falta de confianza en el entorno digital y el incremento de formas de ciber-delincuencia, como el robo de identidad, están obstaculizando el desarrollo de la economía en línea europea. Las tecnologías de identificación electrónica (eID) y los servicios de autenticación son fundamentales para la seguridad de las transacciones electrónicas, tanto en el sector público como en el privado. Actualmente, la manera más corriente de autenticar es utilizar contraseñas, pero cada vez resulta más necesario contar con soluciones más seguras que protejan la intimidad.

Otra barrera a resolver es la eliminación de las fronteras o islas tecnológicas. "Debe hacerse efectivo el concepto de interoperabilidad a todos los niveles y en particular en el caso de la acreditación digital. Debe hacerse efectivo el marco que plantean los Esquemas Nacionales de Seguridad e Interoperabilidad. Pero también Europa necesita una mejor cooperación administrativa para desarrollar e implantar servicios públicos transfronterizos en línea, incluidas unas soluciones prácticas de identificación y autenticación. Es importante avanzar en iniciativas tales como el proyecto piloto a gran escala STORK, que permitan establecer una plataforma europea de interoperabilidad de la identificación electrónica con la finalidad de que los ciudadanos accedan a los servicios de administración electrónica dentro y fuera de su país de origen utilizando su identificación electrónica nacional".

2.10. Tractis

Tractis es una plataforma web que permite negociar, gestionar y firmar contratos 100% online y con plena validez legal en el mundo offline. Tractis permite a particulares y empresas hacer negocios sin importar fronteras, de forma eficiente y con absoluta seguridad y tranquilidad.

Negonation es el nombre de la empresa que está detrás de Tractis. La visión de Negonation es proporcionar justicia transnacional online a la nación internet, creando las herramientas que hagan posible un sistema de justicia alternativo, más eficiente y al alcance de todos. Tractis es el primer paso. Se trata de un desafío enorme que implica estudio de legislaciones, integración con autoridades de certificación y traducción de idiomas a escala global

2.10.1. Entrevista con David Blanco Giró

David Blanco Giró

CEO

Tractis

David Blanco: "No somos sólo tecnología, disponemos de una plataforma exclusivamente de servicios, una característica diferencial respecto a la competencia"

El cofundador de Tractis destaca que ofrecen soporte continuado a más de 70 perfiles de certificados de 28 Autoridades de Certificación en 12 países diferentes.

Para Blanco los ciudadanos valorarán el DNIe sólo cuando puedan realizar con él sus trámites habituales de manera telemática y reconocida tanto en el ámbito público como privado.

En el año 2006 surge el proyecto Tractis, una plataforma de comercio electrónico seguro orientada principalmente al sector privado y con el objetivo claro de convertirse en el PayPal (sistema de pagos y transferencias monetarias a través de Internet) de los contratos. Con esta iniciativa se pone por primera vez a disposición de las pequeñas y medianas empresas una tecnología que, hasta entonces, resultaba prohibitiva para ellas. Pero la visión de la compañía va más allá. "Tractis no es sólo tecnología, sino que ofrece una plataforma de servicios de fácil uso, pero única y exclusivamente de servicios, y esta es nuestra característica diferencial con respecto a la competencia" destaca el cofundador de la

empresa, David Blanco. Con Tractis cualquier persona u organización puede validar certificados, ya sea con propósito de autenticación o de firma, y en la actualidad la empresa ofrece un soporte continuado a 65 perfiles de certificados de 12 países diferentes.

Según explica David Blanco, cuando una organización necesita ofrecer servicios como los de Tractis puede optar por un sistema de *outsourcing* o bien de desarrollo interno. Por lo general se apuesta en la integración con dos o tres autoridades de certificación, dado que la barrera de entrada para llevar a cabo el desarrollo no es elevada, lo que posibilita que se aborde internamente en la empresa. El principal problema reside en el mantenimiento de dichos servicios y sobre todo la apertura a cualquier otro perfil de certificado español, europeo o mundial. "Es ahí donde reside la ventaja competitiva de contar con Tractis como socio tecnológico", apunta Blanco.

Usos del certificado digital

En la actualidad el uso del certificado electrónico en el ámbito privado obedece más a una necesidad competitiva entre las organizaciones del sector que a una necesidad real. Prueba de esta afirmación es el hecho de que todavía no existan proyectos consolidados en este ámbito y, sin embargo, sí se han desarrollado iniciativas muy heterogéneas en cuanto a certificados utilizados o a la limitación en el uso de exploradores para utilizar dichos servicios. "No hay una necesidad todavía clara para pagar por esta tecnología" detalla el responsable de Tractis, al tiempo que recuerda que la actual situación crisis económica también supone un lastre a la hora de impulsar e invertir en este tipo de avances.

Aunque todavía se trabaja para extender el uso y las ventajas del certificado digital, especialmente entre la ciudadanía, hay que destacar el importante papel que España ha jugado y juega a este nivel. España ocupa actualmente un puesto muy relevante respecto al resto de países en materia de implantación de certificación electrónica y, en concreto, del DNIe. "Aunque debemos avanzar en el nivel de utilización del DNIe y de las buenas prácticas para mantenernos en ese liderazgo", apunta David Blanco. En este sentido aborda el distinto ritmo adoptado según cada país para el desarrollo del DNIe.

Así, por ejemplo en Portugal se ofrece la posibilidad de comprar un lector electrónico en el momento de renovar el documento de identidad; mientras que en Estonia, un país reconocido en la Unión Europea por su excelente nivel de buenas prácticas, se incluye el precio del lector en la renovación del DNI, por lo que el usuario se lleva al mismo tiempo un documento renovado y un lector para su uso, ofreciendo además la posibilidad de ser usado en múltiples servicios cotidianos, como los transportes públicos. Sin embargo, España se encuentra en el extremo opuesto, ya que realiza campañas informativas entre los ciudadanos una vez emitido el DNIe, lo que provoca una efectividad mucho menor entre la población que con otra gestión de tiempos y programas. "Esto puede ser una barrera

al uso del certificado electrónico y un freno a la consolidación de España como líder en certificación electrónica", apunta el cofundador de Tractis. En este punto añade que "los ciudadanos verán el valor del DNIe cuando puedan realizar sus transacciones habituales de manera telemática y ello sea reconocido en cualquier entorno, tanto público como privado".

En relación a los usos del DNIe, David Blanco explica que un paso muy importante para el desarrollo de esta iniciativa tecnológica ha sido la liberación de los comandos APDU del DNIe y, aprovechando este cambio, Tractis ha sido pionera en dar soporte a los comandos APDU del DNIe. Esto permite a los clientes de Tractis utilizar su nuevo DNIe sin necesidad de instalar previamente los drivers del DNIe, tarea que por su complejidad, ha dado dolores de cabeza a docenas de miles de ciudadanos.

En la actualidad puede considerarse que todavía se está en la fase de despegue de la implantación del uso del DNIe. De hecho hoy en día aquellas organizaciones que ofrecen servicios mediante este certificado digital, como la banca, tienen todavía un volumen de usuarios muy pequeño con respecto a los usuarios globales.

En este punto, el impulsor de Tractis afirma que el papel que juega la Fábrica Nacional de Moneda y Timbre (FNMT) en esta nueva tecnología no facilita la implantación de servicios de certificado electrónico. Una de las razones es que en estos momentos su OCSP no es de libre consulta, lo que incumple uno de los requisitos que se solicitan para dar firma electrónica reconocida. Por otra parte, los ciudadanos tienen la opción de utilizar el certificado de la FNMT en lugar del DNIe y, como su uso es de momento más sencillo y cómodo, provoca la marginación del DNIe.

"Con la utilización del certificado electrónico existen muchas oportunidades de mejora en los procesos de las organizaciones que las hará ser más competitivas y más eficientes", señala David Blanco. En este sentido apunta al sector de la banca, del que ofrece dos ejemplos representativos como son la creación de cuentas ahorro vivienda los últimos días del año o la formalización de préstamos hipotecarios. En ambos casos el potencial cliente se centra en dos o tres entidades o productos y si el primero que le responde lo hace conforme a mercado existen muchas posibilidades de formalizarlo cuanto antes. "Y en esa estrategia juega un papel importantísimo la agilidad para la firma y, por tanto, poder realizarlo con un certificado electrónico reconocido", añade Blanco. Así, todo el proceso que ahora tarda días e incluso semanas se vería reducido a horas, "lo que cambiaría las reglas de juego". "Y Tractis se centra en estos servicios", concluye.

Retos de futuro

Los avances en materia de implantación y desarrollo de certificación digital han sido muchos en los últimos años, especialmente en materia de fomento del uso del DNIe, como la apertura de comandos APDU. Aún así, todavía se plantean otros muchos retos de futuro en este campo. Uno de los principa-

les, a juicio de David Blanco, es la necesidad de publicar un reglamento que desarrolle la ley de medidas de impulso a la sociedad de la información. Además, apuesta por promocionar que los fabricantes de hardware incluyan en sus productos de serie lectores de DNIe.

Por otra parte sería conveniente incentivar el uso del DNIe frente a los certificados electrónicos personales que emite la FNMT, de tal modo que a largo plazo solamente se tendría un elemento de identificación para los ciudadanos y para los trámites con las Administraciones Públicas.

A nivel global, en la actualidad se está trabajando en proyectos de integración como el Stork, con el que se pretende alcanzar el reconocimiento panaeuropeo de las identidades electrónicas y, en concreto, la aceptación del DNIe y de los identificadores similares en servicios de administración electrónica de otras Administraciones Públicas europeas.

Plan estratégico de Tractis

Uno de los proyectos a corto plazo de Tractis es ofrecer a las Administraciones Públicas los servicios de la empresa de forma gratuita, lo que les facilitaría el cumplimiento de la ley sin ningún tipo de coste o inversión añadida. Además, la visión global de la entidad les lleva a establecer gran parte de su mercado fuera de las fronteras españolas, en países como Méjico o Brasil, con millones de personas que "tarde o temprano acabarán optando por el certificado electrónico y la utilización de los servicios de Tractis".

Consultado sobre las oportunidades de negocio que se abren a través del certificado digital y los productos y servicios asociados, el cofundador de Tractis lo tiene claro: "¿Qué no se haría sin certificado electrónico a largo plazo? Casi nada", afirma, aunque reconoce también todo proceso de renovación tecnológica requiere su tiempo de maduración, y en esta coyuntura se encuentra el certificado electrónico.

3.

SERVICIOS ENTORNO A LA CERTIFICACIÓN DIGITAL

En este apartado se hace un análisis de los servicios y productos ofrecidos actualmente por las organizaciones, públicas y privadas, más representativas en el sector de la certificación digital y la firma electrónica en España.

Aunque se han tenido en cuenta para el estudio muchas organizaciones, para la selección de las entidades analizadas de manera más detallada se han seguido diversos criterios de relevancia como servicios ofrecidos, volumen de certificados gestionados o productos más innovadores. La información incluida en este apartado no pretende ser un catálogo comercial sino ofrecer una visión amplia de los productos y servicios gestionados por los diferentes prestadores de servicios en España.

Todas las organizaciones seleccionadas para el estudio son prestadores de servicios de certificación según lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica. Esta ley establece en su artículo 30, y disposición transitoria segunda, que los prestadores de servicios de certificación deberán comunicar al Ministerio de Industria, Turismo y Comercio, sus datos de identificación, los datos que permitan establecer comunicación con el prestador, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen.

Además, la ley indica que la información deberá ser convenientemente actualizada por los prestadores de servicios de certificación y será objeto de publicación en la dirección de Internet del citado Ministerio con la finalidad de otorgarle la máxima difusión y conocimiento. La dirección de Internet de consulta es la siguiente:

https://www11.mityc.es/prestadores/busquedaPrestadores.jsp

Hay que tener en cuenta que de todos los certificados emitidos y servicios gestionados por los diferentes prestadores de servicios sólo se recogen por el MITyC en su página de registro de prestadores aquellos relativos a la firma electrónica, de persona física y sistemas (las responsabilidades que le asigna la Ley 59/2003 al MITyC sólo abarcan el ámbito de la firma electrónica), así como servicios relacionados como el de sellado de tiempo.

Toda la información analizada en este apartado procede, según lo comentado, de la página WEB del Ministerio de Industria, Turismo y Comercio, y se muestra en este informe de un modo más accesible estructurándose en base a tipos específicos de certificados y servicios.

3.1. Servicios de certificación basados en certificados reconocidos

La relación de prestadores de servicios de certificación que han realizado la comunicación prevista en el artículo 30.2 de la Ley 59/2003 referente a **servicios de certificación basados en certificados reconocidos** son los siguientes:

Servicios de certificación basados en certificados reconocidos
AC ABOGACÍA
ANCERT - Agencia Notarial de Certificación
ANF AC
Autoritat de Certificació de la Comunitat Valenciana - ACCV
BANESTO CA
CAMERFIRMA
CATCert
CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)
CICCP
Dirección General de la Policía y de la Guardia Civil – Cuerpo Nacional de Policía
EDICOM
Firmaprofesional, S.A.
Gerencia de Informática de la Seguridad Social
HEALTHSIGN, S.L.
Izenpe, S.A
Ministerio de Defensa de España
REGISTRADORES DE ESPAÑA
Santander

A continuación se hace una relación de los certificados reconocidos más habituales gestionados por los diferentes prestadores de servicios de certificación:

CERTIFICADOS PARA PERSONAS FÍSICAS

Es el certificado de acreditación de identidad. La entidad certificadora incluye los datos personales en el certificado. Puede solicitarse por internet aunque luego habrá que desplazarse hasta una oficina para acreditar nuestra identidad antes de que se genere el certificado.

Algunos ejemplos de este tipo de certificados son los siguientes:

- **ACCV**: Certificados reconocidos en soporte software para ciudadanos y Certificados reconocidos en dispositivo seguro para ciudadanos (en tarjeta criptográfica)
- **CATCert**: idCAT, idCAT-CEX (ciudadanos no residentes en el Estado español) y CPISR-1
- **FNMT**: Certificado de Persona Física
- **IZENPE**: Certificado de Ciudadano (en tarjeta criptográfica) y Certificado de Asegurado del Sistema Sanitario de Euskadi (suscriptor como asegurado del Sistema Sanitario de Euskadi)

CERTIFICADOS DE FIRMA MÓVIL

Los Certificados de Firma Móvil son certificados digitales de persona física emitidos para ser utilizados desde dispositivos móviles.

Algunos ejemplos de este tipo de certificados son los siguientes:

- **FIRMAPROFESIONAL**: Certificados de Firma Móvil
- **FNMT**: Certificado electrónico para firmar documentos y transacciones con la misma validez legal que la firma manuscrita pero utilizando una tarjeta SIM de telefonía celular

CERTIFICADOS DE REPRESENTANTE

Este tipo de certificados se emiten para personas físicas y determinan la relación de representación legal que ostenta la persona titular del respecto a la entidad o persona jurídica.

Un ejemplo de este tipo de certificados es el siguiente:

- **CAMERFIRMA**: Certificado Cameral de Representante (representación general) y

Certificado Cameral de Persona física de apoderamiento especial (representación especial)

CERTIFICADOS DE PERTENENCIA A ENTIDAD

Los certificados de pertenencia a entidad identifican a las personas que desempeñan cargos o puestos en empresas o entidades.

En este certificado se identifica la empresa o entidad de pertenencia así como en su caso el cargo o puesto desempeñado o la relación de vinculación.

El suscriptor suele ser la persona jurídica o entidad identificada en el certificado y los poseedores de claves las personas físicas que poseen o responden de la custodia de las claves de firma.

Algunos ejemplos de este tipo de certificados son los siguientes:

- **CAMERFIRMA**: Certificado Cameral de Persona Física de pertenencia a Empresa/Entidad
- **CATCERT**: CPISR-1_C, CPISR-2_C (destinados a ser utilizados por cargos de organizaciones ajenas a las administraciones públicas), CPISR-1_CE, CPISR-1_CU (para uso concreto), CPISR-2_E (estudiante) y CPISR-2_EE (estudiante extranjero)
- **FIRMAPROFESIONAL**: Certificado de Colegiado (profesionales colegiados en Colegios Profesionales) y certificado de Persona Vinculada
- **IZENPE**: Certificado Corporativo Reconocido (personas que desempeñan cargos o puestos en entidades públicas que no ejercen potestades administrativas) y Certificado Corporativo Privado Reconocido (en tarjeta criptográfica)

CERTIFICADOS DE FACTURA ELECTRÓNICA

Los Certificados de factura electrónica son certificados digitales expedidos a personas físicas vinculadas a una determinada entidad, destinados a firmar facturas electrónicas en nombre de dicha entidad. Este tipo de certificados son básicamente idénticos a los certificados de pertenencia a empresa o entidad salvo por el hecho de que el suscriptor del certificado está explícitamente autorizado para firmar facturas en nombre de la entidad a la que está vinculado.

Algunos ejemplos de este tipo de certificados son los siguientes:

- **CAMERFIRMA**: Certificado Camerfirma e-Factura
- **FIRMAPROFESIONAL**: Certificado de Factura Electrónica

CERTIFICADO ENTIDAD O DE PERSONA JURÍDICA

Certificados para personas jurídicas emitidos a favor de una entidad que actuará por medio de un representante legal o voluntarios, responsable de las claves, que podrá cederlas para su uso a una tercera persona o aplicativo. Estos certificados permiten a un individuo actuar telemáticamente en representación de una persona jurídica, de acuerdo con lo establecido en el artículo 7 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El grupo de usuarios que pueden solicitar este tipo de certificados está compuesto por los administradores de las entidades, sus representantes legales y voluntarios con poder bastante a estos efectos.

La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante (sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad), cuya identificación se incluirá en el certificado electrónico.

Algunos ejemplos de este tipo de certificados son los siguientes:

- **ACCV**: Certificado reconocido de entidad (en tarjeta criptográfica)
- **CAMERFIRMA**: Certificado Cameral de Persona Jurídica
- **CATCert**: CEISR-1 (en dispositivo seguro de creación de firma) y CEIXSA-1
- **FIRMAPROFESIONAL**: Certificado de Persona Jurídica
- **IZENPE**: Certificado de Entidad

CERTIFICADO DE ENTIDAD SIN PERSONALIDAD JURÍDICA

- Algunos ejemplos de este tipo de certificados son los siguientes:
- **IZENPE**: Certificado de entidad sin personalidad jurídica (en tarjeta criptográfica)

CERTIFICADO DE ÓRGANO ADMINISTRATIVO

Este tipo de certificados identifican al órgano administrativo como firmante y a la persona física titular del mismo y deben ser solicitados por una persona en su propio nombre o en el de una organización. En cualquier caso el suscriptor es siempre el Órgano Administrativo identificado en el certificado.

Estos certificados serán utilizados en el ámbito de las competencias propias del órgano administrativo y del puesto o cargo desempeñado.

Un ejemplo de este tipo de certificados es el siguiente:

- **IZENPE**: Certificado de órgano administrativo (en soporte software)

CERTIFICADOS ELECTRÓNICOS PARA LA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA DE LA ADMINISTRACIÓN PÚBLICA (SELLO ELECTRÓNICO)

Este tipo de certificados tienen por objeto garantizar la identidad y la integridad para la actuación administrativa automatizada. Se encuentran enmarcados en el ámbito de la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios público, y el real decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la misma.

Algunos ejemplos de este tipo de certificados son los siguientes:

- **CAMERFIRMA**: Certificado de sello electrónico para actuación automatizada
- **CATCert**: CDA-1_SENM (sello electrónico de nivel medio de 1024 bits) y CDA-1_SENA (sello electrónico de nivel alto de 2048 bits)
- **FNMT**: Certificado electrónico para la actuación administrativa automatizada de la Administración Pública, organismos y entidades públicas vinculadas o dependientes
- **IZENPE**: Certificado para la actuación administrativa automatizada

CERTIFICADOS ELECTRÓNICOS PARA EL PERSONAL AL SERVICIO DE LAS ADMINISTRA-

CIONES PÚBLICAS

Este certificado tiene por objeto identificar y autentificar tanto al personal al servicio de la Administración Pública como a la Administración Pública misma u órgano en la que presta sus servicios. Se encuentra enmarcado en el ámbito de la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios público, y el real decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la misma.

Algunos ejemplos de este tipo de certificados son los siguientes:

- **ACCV**: Certificado reconocido en dispositivo seguro para empleados públicos (en tarjeta criptográfica)
- **CAMERFIRMA**: Certificado de empleado público
- **FNMT**: Certificado electrónico para el personal al servicio de las Administraciones Públicas
- **IZENPE**: Certificado de Personal de las Entidades Públicas (en tarjeta criptográfica) y Certificado de Personal del Gobierno Vasco (en tarjeta criptográfica)

3.2. Servicios de certificación basados en certificados no reconocidos

La relación de prestadores de servicios de certificación que han realizado la comunicación prevista en el artículo 30.2 de la Ley 59/2003 referente a **servicios de certificación basados en certificados no reconocidos**:

Servicios de certificación basados en certificados no reconocidos
CAMERFIRMA
CATCert
CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)
Colegio Oficial de Arquitectos de Sevilla
ipsCA
Izenpe, S.A
Ministerio de Defensa de España
Servicio de Salud de Castilla-La Mancha (SESCAM)
Telefónica Empresas.

A continuación se hace una relación de los certificados no reconocidos más habituales gestionados por los diferentes prestadores de servicios de certificación:

CERTIFICADO DE DISPOSITIVO APLICACIÓN

Este tipo de certificados se utilizan para, almacenados en un servidor (es un certificado de componente que está asociado normalmente a una clave custodiada por una máquina) y requeridos por una aplicación, firmar documentos o mensajes. Estos certificados se emiten a personas jurídicas responsables de la operación de aplicaciones informáticas que se identifican digitalmente, firman electrónicamente webservices u otros protocolos y que reciben documentos y mensajes cifrados.

Son certificados ordinarios, y que garantizan la identidad de la persona responsable y la integridad y la autenticidad de los datos firmados. También permiten la recepción de información cifrada.

Algunos ejemplos de este tipo de certificados son los siguientes:

- **CAMERFIRMA**: Certificado de sello de empresa
- **CATCert**: CDA-1

CERTIFICADO DE PERSONA JURÍDICA Y ENTIDADES SIN PERSONALIDAD JURÍDICA

Un ejemplo de este tipo de certificados es el siguiente:

- **FNMT**: Certificados no reconocidos de persona jurídica y entidades sin personalidad jurídica (para el ámbito tributario)

CERTIFICADOS DE PERTENENCIA A EMPRESA

El suscriptor será la persona jurídica identificada en el certificado y los poseedores de las claves las personas físicas que poseen o responden de la custodia de las claves de firma. Un ejemplo de este tipo de certificados es el siguiente:

- **IZENPE**: Certificado privado no reconocido (en tarjeta criptográfica)

CERTIFICADOS DE PERTENENCIA A ENTIDAD PÚBLICA

Es el certificado en que se identifica a personas que desempeñan cargos o puestos en entidades públicas que no ejercen potestades administrativas. Se trata de un certificado en el que el suscriptor será necesariamente la misma entidad usuaria. En este certificado se incluye la entidad pública de pertenencia así como, en su caso, el cargo desempeñado. Un ejemplo de este tipo de certificados es el siguiente:

- **IZENPE**: Certificado corporativo no reconocido

3.3. Servicios en relación con la firma electrónica

La relación de prestadores de servicios de certificación que han realizado la comunicación prevista en el artículo 30.2 de la Ley 59/2003 referente a **otros servicios en relación con la firma electrónica**:

Otros servicios en relación con la firma electrónica - Servicios de validación temporal
ANF AC
Autoritat de Certificació de la Comunitat Valenciana - ACCV
CAMERFIRMA
CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)
EADTrust
EDICOM
Firmaprofesional, S.A.
Gerencia de Informática de la Seguridad Social
Izenpe, S.A
Ministerio de Defensa de España
Tractis

Otros servicios en relación con la firma electrónica - Servicios de validación de certificados
CertiVer
EADTrust
Tractis

Otros servicios en relación con la firma electrónica - Servicios de custodia
CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)
Tractis

Otros servicios en relación con la firma electrónica - Otros servicios
CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)
EDICOM
Firmaprofesional, S.A.
Izenpe, S.A

A continuación se hace una relación de los servicios más habituales gestionados por los diferentes prestadores de servicios de certificación en este ámbito:

SERVICIO DE SELLADO ELECTRÓNICO

El sellado electrónico de documentos o timestamping es el complemento ideal de la firma electrónica ya que es un sistema por el que un tercero asegura que los datos contenidos en un documento existen desde una fecha concreta.

La firma electrónica adolece de este defecto, y es que no tenemos la certeza de cuando se ha firmado el documento electrónico. Para cierto tipo de contratos la fecha no es un dato esencial, pero para otros como puede ser la contratación de un seguro, se convierte en algo tan importante como la misma firma. Lo mismo podemos establecer para un contrato de servicio o para sellar una reclamación, como puede ser ante la administración.

Se trata, por lo tanto, de la emisión de sellos de tiempo que permitan asociar una actuación con una fecha y hora, y así obtener evidencias técnicas y jurídicas de que tal acto que se ha producido en un determinado momento de tiempo.

Algunos ejemplos de este tipo de servicio son los siguientes:

- **ACCV**: Servicio de sellado de tiempo (generación y emisión de sellos de tiempo para organismos de la Generalitat Valenciana, así como para cualquier otra administra-

ción o entidad pública con la que se haya firmado el correspondiente convenio de certificación)

- **CAMERFIRMA**: Sellado de tiempo
- **EADTrust**: Servicio de sellado de tiempo
- **FIRMAPROFESIONAL**: Servicio de sellado de tiempo
- **FNMT**: Servicio de Timestamping
- **IZENPE**: Servicio de sellado de tiempo
- **TRACTIS**: Servicio de sellado de tiempo

SERVICIO CONSTANCIA Y ACREDITACIÓN DE LA PUBLICACIÓN

Este servicio sirve para actuar como Tercero de Confianza de modo que de fe de la publicación a partir de un determinado momento en el tiempo y que hasta otra fecha determinada dicha publicación no ha sido modificado ni ha permanecido accesible.

De este modo cualquier entidad, pública o privada, podrá contar un tercero que demuestre fehacientemente que un documento ha sido publicado y ha permanecido inalterado y accesible en el tiempo.

Un ejemplo de este tipo de servicio es el siguiente:

- **IZENPE**: Servicio de Constancia y Acreditación de Publicación

SERVICIO DE CUSTODIA DE DOCUMENTOS ELECTRÓNICOS

La custodia de las transacciones y documentos electrónicos es un factor importante en el desarrollo de las relaciones electrónicas entre partes ya que permiten dotar a las mismas de seguridad jurídica preventiva preconstituyendo tanto una prueba testimonial como documental de la realización de la transacción entre las partes. El servicio de custodia de documentos electrónicos es un servicio, cuyo acceso se realiza mediante identificación por procedimientos de firma electrónica. El servicio provee a los clientes de un sistema de depósito de documentos electrónicos realizado por un tercero capaz de dar fe de la existencia y contenido del documento.

Un ejemplo de este tipo de servicio es el siguiente:

- **FNMT**: Servicio de Custodia de Documentos Electrónicos

SERVICIO DE VALIDACIÓN DE CERTIFICADOS

Se trata de servicios que proporcionan información acerca del estado de validez de diferentes tipos de certificados emitidos por uno o varios Prestadores de Servicios de Certificación (servicios semejantes a los que **@firma** presta en el sector público).

Algunos ejemplos de este tipo de servicio son los siguientes:

- **EADTrust**: Servicio de validación de certificados
- **Tractis**: Servicio de autoridad de validación semántica

3.4. Otros servicios

Como se ha comentado anteriormente, hay que tener en cuenta que de todos los certificados y productos ofrecidos por los diferentes prestadores de servicios de certificación sólo se recogen por el MITyC, en su página de registro de prestadores, aquellos relativos a la firma electrónica, de persona física y sistemas, así como servicios relacionados como el de sellado de tiempo. Estos certificados y servicios han sido analizados en los apartados 3.1, 3.2 y 3.3 de este informe.

En este apartado se analizan otros servicios ofrecidos por los prestadores de servicios al margen de los relacionados estrictamente con la firma electrónica y el sellado de tiempo.

3.4.1. Certificados

CERTIFICADO DE SEDE

Los certificados reconocidos de Sede Electrónica sirven para identificar un portal WEB y establecer comunicaciones seguras, de tal forma que se garantiza la privacidad e integridad de la información que se ofrece, excluyendo la posibilidad de ser víctimas de un fraude.

La Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos define la Sede Electrónica como la dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

Las Sedes Electrónicas deben dotarse de herramientas criptográficas:

- Identificar al sitio web y su vinculación con una determinada Administración Pública
- Garantizar la privacidad de las comunicaciones, es decir, que la información intercambiada entre un ciudadano usuario de esa Sede y la propia Sede sea cifrada
- La autenticación o identificación de las sedes electrónicas se realizará mediante la utilización de certificados digitales de sede electrónica (Artículo 18 Real Decreto 1671/2009).

El certificado reconocido de Sede Electrónica básicamente es un certificado de servidor WEB seguro que incluye la identificación del titular de la Sede Electrónica, y que se emite en un dispositivo seguro o medio equivalente.

Algunos ejemplos de este tipo de certificado son los siguientes:

ACCV: Certificado de Sede Electrónica

CAMERFIRMA: Certificado de Sede Electrónica

CARCert: Certificado de Sede Electrónica

FIRMAPROFESIONAL: Certificado de Sede Electrónica

FNMT: Certificado de Sede Electrónica

IZENPE: Certificado de Sede Electrónica y Sede Electrónica con EV (validación extendida que aporta mejoras de protección al usuario)

CERTIFICADOS DE CLIENTE SEGURO

Son certificados empleados para identificar y autenticar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.

CERTIFICADOS DE SERVIDOR SEGURO

Son certificados empleados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.

CERTIFICADOS DE FIRMA DE CÓDIGO

Los certificados de firma de código son una herramienta cada vez más utilizada por los desarrolladores para la firma electrónica de aplicativos.

La firma electrónica de código permite distribuir de forma segura ActiveX, Macros, Applets, MIDlet (J2ME) garantizando la autenticidad e integridad del contenido antes de ser ejecutado, y de esta forma eliminando riesgos

3.4.2. Productos y soluciones

En este apartado se analizan algunos productos y soluciones en torno a la firma electrónica

de especial interés:

3.4.2.1. Servicios de validación de certificados digitales

Este tipo de servicios permiten la consulta del estado de los certificados. El validador responde si un certificado es válido o no es válido (por ejemplo, porque está revocado) y en la misma respuesta también devuelve información adicional, como por ejemplo, datos útiles del certificado digital (por ejemplo el nombre y apellidos, el DNI, etc.) y el nivel de seguridad asociado al certificado digital.

Generalmente este tipo de servicios reconocen múltiples prestadores de servicios de certificación, uniformizando la información asociada a los certificados, soportan los mecanismos de validación de certificados estándares y admite la integración de cualquier otro mecanismo personalizado.

Las **lista de certificados revocados (CRL)** contienen el número de serie de todos los certificados emitidos por una Autoridad de Certificación y que, por algún motivo han dejado de ser válidos de manera previa a la expiración de su periodo de validez original. Para saber si un certificado es de confianza debe comprobar si el número de serie del mismo está incluido en la CRL publicada por la Autoridad de Certificación emisora. Si es así, el certificado ha sido revocado y no es de confianza.

Los **servicios OCSP (Online Certificate Status Protocol)**, definidos en el estándar RFC-2560, proporcionan a los usuarios y las aplicaciones un método ágil y rápido de obtener el estado de un certificado, evitando tener que descargar la Lista de Certificados Revocados (CRL).

3.4.2.2. Servicios de validación de firmas digitales

Este tipo de servicios permiten realizar comprobaciones sobre la validez de una firma digital. El servicio inspecciona la firma y verifica por una parte que la firma esté bien formada y por otra parte, comprueba el estado del certificado en el momento que se ha producido la firma. En función de los resultados anteriores responde si la firma es válida o no es válida.

3.4.2.3. Firma electrónica en aplicaciones

Generalmente son componentes software (applets o similares) que facilitan la integración de la funcionalidad de firma electrónica en aplicaciones web, y que permite firmar diferentes formatos de documentos y con diferentes formatos de firma

3.4.2.4. Preservación y archivo electrónico de documentos

Se trata de servicios que garantizan que los documentos que genera o recibe una organización en el ejercicio de sus funciones se mantienen íntegras, fiables, auténticos y accesibles a lo largo de su ciclo de vida.

Este tipo de servicios incluye generalmente:

La creación de una plataforma tecnológica de archivo digital o repositorio para almacenar los documentos electrónicos que pueda garantizar a lo largo del tiempo la autenticidad, la fiabilidad, la integridad, la seguridad y la disponibilidad de los documentos electrónicos y su información.

El desarrollo de estrategias o soluciones tecnológicas para tratar los problemas derivados de la durabilidad de los soportes y la obsolescencia de la tecnología.

La implantación de un sistema de gestión de la información es clave para optimizar los procesos y mejorar el servicio ofrecido y la seguridad de la información

La custodia de documentos es un paso más en la gestión documental e implica la existencia de un tercero que se responsabiliza de archivar, con garantías técnicas y legales, los documentos de otras organizaciones.

Existen diversas entidades y empresas que ofrecen el servicio de custodia de información basado en el almacenamiento de documentos, tanto firmados digitalmente y/o cifrados como sin firmar y/o cifrar y garantizando que el documento custodiado mantiene a lo largo del tiempo el mismo valor legal.

Para mantener la validez legal en el tiempo se define, en función de los diferentes plazos de custodia (corto, medio y largo plazo), la tecnología y los soportes a utilizar así como los formatos aceptados y su mantenimiento. Además, generalmente, se incorpora un sellado de tiempo en los documentos firmados que asegura el momento de realización de la firma y la validez del certificado con el que se realizó la misma.

3.4.2.5. Bróker de identidades

Los **bróker de identidades** son "agentes mediadores" que se ocupan de facilitar información asociada con la identificación de un ciudadano que no obre en poder de aquél que gestiona el servicio.

En una sociedad con ciudadanos desarrollando trámites o actividades en diversos municipios o entidades frente a las posibles necesidades informativas es precisa la comunicación entre ellas, así como que se establezcan convenios de colaboración entre ellas. Los *brokers*

de identidades surgen para realizar las labores de intermediación entre las entidades de modo que para aquellas que quieran llamar a servicios a través de esta plataforma las llamadas sean siempre con el mismo formato independientemente del proveedor del servicio. Además permiten la solicitud de un servicio a varias entidades a la vez o la relación con otros agentes de intercambio.

3.4.2.6. Facturación electrónica

La **facturación electrónica** es un equivalente funcional de la factura en papel y consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos. Dependiendo del volumen de las empresas, el ahorro por concepto de administración de facturas (recepción, almacenaje, búsqueda, firma, devolución, pago, envío, etc.) puede fluctuar entre el 40% y el 80%.

En un sistema de facturación electrónica, por cada factura intercambiada se debe adjuntar la firma electrónica de la misma, generada con los datos de firma del emisor, y todos los datos que permitan al receptor verificar la integridad de lo firmado y la autenticidad del firmante. Los algoritmos criptográficos utilizados tanto para el hash del documento como para la firma electrónica deben estar plenamente aceptados por la comunidad internacional (SHA1, MD5, RSA etc.).

El receptor de la factura electrónica deberá disponer del software que permita verificar la firma de la factura y la identidad del emisor, así como que el certificado utilizado para la generación de la firma electrónica es válido (no está revocado ni caducado).

Existen en el mercado diferentes soluciones para aquellas empresas y trabajadores autónomos que deseen realizar la facturación electrónica de una forma fácil. Estas soluciones, que sirven para realizar tareas tales como crear, firmar o enviar facturas, están orientadas a usuarios que no dispone de conocimientos avanzados para esta tarea.

La facturación electrónica requiere de certificados de firma digital necesarios para poder emitir una factura para que esta tenga validez. Los certificados digitales válidos para la emisión de facturas electrónicas deben:

Seguir el estándar UIT X.509 versión 3 o superior

Estar emitidos por una Autoridad de Certificación admitida en las relaciones tributarias por medios electrónicos y telemáticos con la Agencia Estatal de Administración Tributaria (AEAT)

4.

ANÁLISIS DE LA LEGISLACIÓN ACTUAL

En este apartado se desarrolla un amplio análisis de la legislación actualmente vigente en materia de identidad digital y firma electrónica.

Para la elaboración de este apartado se ha contado con la colaboración del abogado Víctor Salgado Seguín del bufete Pintos & Salgado Abogados. El bufete Pintos & Salgado Abogados, especializado en la aportación de soluciones jurídicas en el ámbito de las nuevas tecnologías, cuenta con más de diez años de experiencia en consultoría legal informática, propiedad intelectual y auditoría e implantación de la normativa de protección de datos de carácter personal.

4.1. Marco general

No nos queda más remedio que admitir que estamos demasiado apegados a la tinta y al papel. Hemos crecido con estos medios y, por tanto, le atribuimos la máxima credibilidad. Históricamente, todo lo que podemos tocar e, incluso, oler, nos aporta mucha más seguridad sobre la fiabilidad y realidad de las cosas.

Es verdad que en muchas ocasiones es conveniente, e incluso necesario, que exista una prueba documental escrita a efectos de verificar la existencia de una relación jurídica o de un hecho determinado, ya sea por su importancia intrínseca o ya por exigencia legal. Sin embargo, debemos percatarnos que en el mundo digital que nos rodea, y gracias a nuestra nueva legislación que tendremos oportunidad de comentar, el que algo conste "por escrito" no será nunca más sinónimo de necesariamente "en papel". Más bien todo lo contrario.

Una de las primeras normas que lo han hecho posible fue el, ya derogado, Real Decreto-Ley 14/1999, de 17 de septiembre, por el que se reguló por vez primera la Firma Electrónica en nuestro país. Con esta regulación, España se convirtió en uno de los primeros países, a nivel mundial, en reconocer legalmente la validez de un documento electrónico firmado digitalmente.

La firma electrónica, como veremos, es un medio de prueba incluso más seguro y fiable como prueba que la familiar firma manuscrita. Esto es debido a que, gracias a la magia de su tecnología, la misma no sólo nos va a indicar "quién firma" sino también "lo que firma" ya que, como gran novedad, se vincula al propio texto del documento a firmar (lo cual en papel es imposible).

Sin embargo, a pesar de este temprano reconocimiento jurídico y de sus grandes ventajas para la seguridad probatoria, lo cierto es que su uso en la práctica ha sido desalentadoramente marginal.

A pesar de ello, algunos servicios y trámites como la declaración de impuestos a través de Internet han sido una honrosa excepción y un exitoso ejemplo de una amplia implantación e indudable utilidad de la firma electrónica en nuestro país. A fin de que este ejemplo pueda generalizarse, el Parlamento aprobó una serie de normas destinadas, no solo a ampliar su reconocimiento sino especialmente a fomentar su uso. Destacamos especialmente tres:

En primer lugar, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, por la que se reconoce por vez primera la equivalencia jurídica de la palabra "escrito" a la palabra "electrónico", hablando de contratos y siempre que se garantice su prueba mediante soporte digital.

En segundo lugar, la Ley 59/2003, de 19 de diciembre, de firma electrónica, que sustituyó la citada norma del 99, contempló, entre otras novedades, la creación del DNI digital, con la consiguiente generalización de la tenencia (que no del uso) de la firma electrónica en nuestro país.

Y, en tercer lugar, Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que garantiza el derecho de todos a relacionarnos con las Administraciones Públicas a través de medios electrónicos y, principalmente, a través del uso de la firma electrónica legalmente reconocida.

A continuación, daremos un rápido repaso a los aspectos fundamentales de esta normativa:

4.2. Hacia la identidad digital

Como hemos comentado, desde 1999 España fue pionera en legislar sobre la firma electrónica. Actualmente, la misma ya se reconoce en la práctica totalidad de países desarrollados y, en nuestro país, se regula ahora mediante la Ley 59/2003, de 19 de diciembre, de firma electrónica.

A pesar de ello, es aún una gran desconocida para la gran mayoría de los ciudadanos. Por ejemplo, si preguntáramos a un grupo amplio de personas cuántos tienen firma electrónica, seguramente responderían muy pocos afirmativamente. Hace poco, hicimos este pequeño experimento con alumnos en la universidad y, a esta pregunta, menos de un 5% levantaron la mano positivamente.

Por otro lado, si preguntamos cuántos han renovado recientemente su DNI, sin duda contestarán muchos más afirmativamente. Cuando repetimos esta misma pregunta en la universidad, levantaron la mano casi un 50% de los asistentes.

Pues, repito lo mismo que les dijimos en su día a nuestros alumnos: "los segundos deberíais haber levantado la mano al principio. Lo sepáis o no, vuestro reciente DNI (ese que tiene un pequeño chip como la tarjeta del Bus) incorpora ya vuestra firma electrónica en el mismo. Por tanto, ¡ya tenéis firma electrónica!".

Por tanto, sólo tenemos que ser conscientes de ello.

¿Dónde podremos usarla?

Pues es un gran número de transacciones en Internet. Con el tiempo serán prácticamente las mismas que en el mundo físico.

Esto es debido, entre otras normas, también al artículo 23 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), en base al cual serán válidos todos los contratos que realicemos a través de la Red, incluso los que la Ley exija "por escrito":

"1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico,(…).

3. Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico."

De hecho, los únicos ámbitos que quedan exceptuados de lo anterior son los siguientes:

Los contratos relativos al Derecho de familia y sucesiones.

Los documentos y escrituras públicas.

Por supuesto, el DNI Digital no es la única firma electrónica válida en nuestro país. Hay muchas otras reconocidas que son emitidas por empresas y entidades de todo tipo para su uso en distintos ámbitos cumpliendo los requisitos estipulados en la Ley.

A continuación veremos los aspectos básicos de dicha normativa.

4.3. La firma electrónica (Ley 59/2003)

Concepto y Tipos de Firma Electrónica

De acuerdo, hemos hablado de sus ventajas y virtudes jurídicas pero, ¿qué es la firma electrónica?

El artículo 3.1 de la Ley 59/2003 de Firma Electrónica, la 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".

Sin duda, es una definición bastante ambigua pero que ya nos define los tres elementos principales de la firma electrónica:

Es un "conjunto de datos" en formato digital, pudiendo componerse de texto, números u otros símbolos;

Que están situados junto a otros, que supondrían el "texto o datos firmados", pudiendo incluso estar asociados con ellos (ya sea mediante fórmulas matemáticas o de otro modo) y

Que pueden identificar al firmante: éste, sin duda, es el elemento clave y todo el texto de la Ley se encamina a reforzar esta identificación de modo único y válido jurídicamente.

Pero ¿todas las firmas electrónicas son iguales?

Obviamente, no. Dependerá de diversos factores que influirán en su mayor o menor reconocimiento y validez probatoria.

De este modo, el artículo 3 de la ley nos habla también de los diversos tipos de firma electrónica. Define, fundamentalmente cuatro tipos:

La firma electrónica avanzada;

La firma electrónica reconocida;

La firma electrónica no reconocida y

Finalmente, la que denominaremos como "firma electrónica acordada".

Vamos a ver rápidamente cada uno de estos cuatro tipos de firma electrónica:

La firma electrónica avanzada

La firma electrónica avanzada se define como aquélla que cumple los siguientes requisitos:

Permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados;

Está vinculada al firmante de manera única y a los datos a que se refiere; y

Ha sido creada por medios que el firmante mantiene bajo su exclusivo control.

Aunque la ley, obviamente, no puede decantarse por uno u otro tipo de tecnología concreta debido al principio de neutralidad tecnológica, es evidente que la firma electrónica avanzada se refiere a la tecnología ampliamente utilizada y difundida en la actualidad de "criptografía de clave asimétrica".

Esto se deduce de los elementos identificativos que acabamos de resumir. El primero de ellos, se refiere a que no sólo debe permitir identificar al firmante sino que además dicha firma debe detectar cualquier cambio posterior en los datos firmados. Ésta es una característica fundamental de la criptografía de clave asimétrica, que se define como "integridad" de la firma y que es debida, a que la misma va vinculada al texto sobre el cual se está aplicando. Ello significa que cualquier alteración posterior del texto o datos firmados en primera instancia, aunque fuera de "una sola coma", supondrá un error, ya no de la firma en sí misma, sino de su aplicación sobre los datos firmados.

Os pondré un ejemplo práctico:

Si yo os pidiera que me firmaseis un autógrafo en un papel en blanco (por si un día sois famosos), sin duda muchos no tendríais reparos en hacerlo.

Ahora bien, si yo os dijera que en dichos papeles posteriormente imprimiré lo siguiente: "Yo, fulano de tal, por la presente declaro que le debo 5.000 euros a mengano en concepto de préstamo personal el cual será devuelto a su solicitud" ¿Cómo probaríais que dicho documento es falso?

Lo cierto es que lo tendríais muy difícil puesto que la prueba más extendida para ello es la pericial caligráfica sobre vuestra firma, y dicha prueba diría que efectivamente la misma es vuestra.

Es decir, en papel no hay modo de saber qué estaba escrito en el momento de la firma (al menos de manera sencilla).

Sin embargo, esto no ocurre con la firma electrónica avanzada. De hecho, la misma se genera a partir del texto que estamos firmando. De este modo, si alguien cambiara o añadiera una sola coma al documento electrónico firmado, dicha firma sería inválida: una prueba sencilla nos diría que sí es nuestra firma pero que no es el texto que firmamos originalmente.

Esto es lo que llamamos "integridad" de la firma electrónica y en Derecho es como descubrir la piedra filosofal que puede acabar con todas las falsedades documentales y au-

mentará, por tanto, la seguridad jurídica de los documentos electrónicos por encima de sus homólogos en papel.

La firma electrónica reconocida

Esta firma es la única firma electrónica cuyo valor jurídico y probatorio se equipara plenamente a la firma manuscrita en la ley.

En realidad, es una firma electrónica avanzada que además cumple las características siguientes:

Estar basada en un "certificado reconocido" y

Estar generada por un "dispositivo seguro de creación de firma".

Estos dos elementos adicionales confieren a esta firma una seguridad jurídica completa.

Pero, ¿qué es un certificado?:

El artículo 6.1 de la Ley de Firma Electrónica define al certificado electrónico 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".

Éste documento tiene una importancia vital puesto que relaciona de manera inequívoca a una clave pública concreta con su poseedor legal y confirma plenamente su identidad. Sin esta confirmación documental, no tendríamos manera de saber si la persona que aparece como titular de la clave es, en realidad, su propietaria.

Dicho documento deberá ir firmado, a su vez, por un "tercero de confianza" o, como lo denomina la ley, un prestador de servicios de certificación. Este prestador deberá establecer algún mecanismo para verificar dicha identidad además de someterse a un régimen de responsabilidad concreto sobre dicha identificación.

Esto en cuanto a un certificado electrónico, pero ¿qué es un "certificado reconocido"?

El artículo 11.1 de la Ley define al certificado reconocido como aquel certificado electrónico expedido por un prestador de servicios de certificación que cumpla uno requisitos especiales, precisamente, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y, por otro lado, a la fiabilidad y las garantías de sus servicios.

Entre otros requisitos, el artículo 20.2 de la Ley establece la obligación de contar con un seguro de responsabilidad civil de 3 millones de euros para responder por su actividad.

La firma electrónica no reconocida

Éste tipo de firma es especialmente importante en lo que se refiere a la validez jurídica última de otros tipos posibles de firma electrónica distintos a los que acabamos de analizar.

Así, el artículo 3.9 de la Ley de Firma Electrónica, determina que "no se le 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".

Esto supone, a la postre, un reconocimiento implícito de la validez jurídica de otros tipos de firma electrónica, siempre y cuando estemos en disposición de probar su correcta emisión, vinculación, configuración y solidez técnica y jurídica.

Todo ello, deberá ser acreditado, en su momento, por el titular, firmante o parte interesada dentro de un procedimiento legal.

La firma electrónica acordada

El apartado 10 del artículo 3 de la Ley de Firma Electrónica incorpora un último tipo de firma que nosotros hemos denominado como "firma electrónica acordada".

Este apartado dispone que: "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".

Esto significa que, cualquiera que fuera el sistema de firma electrónica que se utilizara, si dicho sistema fuera convenido o acordado por las partes de un contrato, el mismo tendría plena validez jurídica y probatoria entre las mismas, siempre y cuando se cumplan los requisitos estipulados en dicho contrato.

Esto abre la vía para que sistemas menos formales o convencionales puedan tener pleno valor probatorio en ámbitos cerrados o con un número limitado de intervinientes.

El DNI digital

Como adelantábamos anteriormente, el artículo 15 de la Ley de Firma Electrónica, define al Documento Nacional de Identidad Electrónico como aquel documento que:

Por un lado, acredita electrónicamente la identidad personal de su titular y,

Por otro lado, permite asimismo la firma electrónica de documentos.

La gran importancia que tiene la emisión de este nuevo documento nacional de iden-

tidad, es que, el propio artículo 15, dictamina que "todas las personas físicas o jurídicas, públicas o privadas, deberán reconocer su eficacia".

Por tanto, el documento nacional de identidad electrónico es la única firma electrónica reconocida que lo es simplemente por su mero reconocimiento expreso en la propia ley.

Para usarla, sin embargo, se necesita un lector especial del chip que lleva el propio DNI. Los ordenadores deberían traerlos de serie en breve pero, mientras tanto, se pueden comprar en tiendas especializadas por un precio asequible, acogiéndonos a ofertas periódicas de los proveedores con precios reducidos o, incluso, de modo gratuito como medidas de impulso del uso del DNIe subvencionadas por el Gobierno.

Hoy en día, cada vez son más los servicios de Internet donde podemos utilizar el DNIe: principalmente en el ámbito de las administraciones públicas (Hacienda, Seguridad Social, Ayuntamientos, etc.) pero también comienza a introducirse en el ámbito privado donde podemos ver ya algunos Bancos y Cajas de ahorro que lo utilizan como forma alternativa a sus tradicionales (y, en ocasiones, menos seguras) claves de acceso.

Validez probatoria, aplicación y usos

Como hemos visto, hoy en día ya se admite la plena validez jurídica de la firma electrónica a un mismo nivel incluso que la firma manuscrita, pero ¿qué documentos se pueden firmar digitalmente?

Lo cierto es que, gracias a nuestra avanzada legislación, son ya prácticamente todos:

Todo tipo de contratos, incluso los que se exijan en "forma escrita", a excepción de los de familia, sucesiones y escrituras públicas. (como vimos, gracias al artículo 23 de la LSSICE).

Las facturas, siempre que se cumplan los requisitos establecidos en la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso a la Sociedad de la Información (LMISI) y normativa concordante.

Declaraciones y documentos para las Administraciones Públicas, posible desde hace años en el ámbito fiscal o laboral pero con un impulso importante a partir de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).

Y, en definitiva, todos aquellos otros documentos respecto de los cuales no se hayan regulado requisitos formales para su validez.

Y, en su caso, ¿cómo se puede presentar una firma electrónica como prueba en un procedimiento?

El artículo 3. 8 de la Ley de Firma Electrónica dispone que "el soporte en que se hallen los

datos firmados electrónicamente será admisible como prueba documental en juicio".

Esto significa que cualquier persona o parte interesada en un procedimiento judicial podrá aportar cualquier documento directamente en formato digital o electrónico como prueba documental en juicio sin que se le pueda exigir su transposición a cualquier otro soporte no digital. Por ejemplo, impresión en papel u otro sistema análogo.

4.4. Las Administraciones Públicas frente al ciudadano digital (Ley 11/2007)

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos dispone que todas las Administraciones Públicas deberán estar plenamente accesibles en la Red para los ciudadanos.

En base a ello, cualquier procedimiento, servicio o trámite prestado por un Ayuntamiento, una Comunidad Autónoma o un Ministerio, deberá estar también disponible por medios electrónicos.

Así, el artículo 6.1 de la citada Ley 11/2007, también denominada como Ley de Administración Electrónica (LAE), regula el acceso electrónico de los ciudadanos a los Servicios Públicos como un verdadero derecho de los ciudadanos:

"Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos (…), así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos."

Entre otros, la LAE nos reconoce igualmente los siguientes derechos:

A no volver a aportar los datos y documentos que ya obren en poder de las Administraciones Públicas.

A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que seamos interesados.

A obtener copias electrónicas de los documentos electrónicos que formen parte de dichos procedimientos.

La digitalización de documentos y el uso generalizado de Internet en los procedimientos administrativos conllevará un importante ahorro del gasto público (menos papel, menos locales destinados a archivo, menos costes de transporte, burocracia más ligera, trámites automatizados que reducirán los gastos extra de personal, y un largo etcétera).

Estas ventajas son paralelas de los igualmente importantes beneficios para el ciudadano: menos gastos en desplazamientos (muchas veces inútiles) y correveidiles de una ventanilla a otra; ahorro de tiempo derrochado en esperas de interminables colas; evitar el "vuelva usted mañana" con horarios amplios para presentar una solicitud o un documento a las 12:00 de un domingo; más comodidad, etc.

Surgen nuevas necesidades: la identificación y autenticación en la Administración Electrónica

Ante la necesidad de concretar lo dispuesto en la LAE, se adoptó 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.

Este Real Decreto, cuyo ámbito se circunscribe a la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta, tiene por objeto desarrollar la LAE en todo lo relativo a la transmisión de datos, sedes electrónicas y punto de acceso general, identificación y autenticación, registros electrónicos, comunicaciones y notificaciones y documentos electrónicos y copias.

Es en concreto el Capítulo I de su Título III el que aborda todo lo relativo a la identificación y autenticación en el acceso electrónico de los ciudadanos a dicha administración y órganos dependientes. Así, el artículo 10.1 dispone que: "Las personas físicas podrán utilizar para relacionarse electrónicamente con la Administración General del Estado y los organismos públicos vinculados o dependientes, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, en todo caso, y los sistemas de firma electrónica avanzada admitidos".

Una vez más, vemos la admisión preferente del DNIe frente a otros tipos de firma electrónica que, sin ser limitados estrictamente a la firma electrónica reconocida, sin embargo deben ser aceptados por la administración. Esto se hace patente especialmente en lo referente a otros sistemas de firma electrónica (especialmente los no criptográficos), los cuales deberán aprobarse mediante Orden Ministerial o incluso mediante acuerdo del Consejo de Ministros, previo informe del Consejo Superior de Administración Electrónica, en base a lo dispuesto en el artículo 11 del Real Decreto 1671/2009.

Este Real Decreto dispone también el régimen especial de habilitación para la representación de terceros y crea el Registro electrónico de apoderamientos para actuar electrónicamente ante la Administración General del Estado y sus organismos públicos dependientes o vinculados, regulado en su artículo 15.

Finalmente, el artículo 16 desarrolla la identificación y autenticación de los ciudadanos, cuando fuera necesaria, de forma personal ante funcionarios públicos especialmente habilitados, los cuales deberán de contar con una firma electrónica aceptada y estar en un registro especial que mantendrá el Ministerio de la Presidencia y cuyas funciones se podrán extender a otras Administraciones Públicas Mediante convenio.

Esto en lo relativo a la Administración General del Estado; ¿y que hay de Galicia?

Pues, por su parte, nuestra Comunidad Autónoma, ha aprobado recientemente el Decreto 198/2010, de 2 de diciembre, por el que se regula el desarrollo de la Administración

electrónica en la Xunta de Galicia y en las entidades de ella dependientes. Su Capítulo IV es el encargado de regular todo lo relativo a la identificación y autenticación ante dicha administración autonómica.

En concreto, su artículo 14.2 dispone que "los ciudadanos podrán utilizar los siguientes instrumentos de identificación para relacionarse con la Xunta de Galicia y las entidades incluidas en el ámbito de aplicación de este decreto:

En todo caso, los sistemas de firma electrónica incorporados al documento nacional de identidad, para personas físicas.

Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las administraciones públicas que tengan validez para la Xunta de Galicia y que se especifiquen en la sede electrónica.

Sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como persona usuaria inscrita en el registro de funcionarios habilitados por la Xunta de Galicia.

Otros sistemas de identificación que resulten proporcionales y seguros para la identificación de las personas interesadas."

Como podemos comprobar, se sigue el mismo esquema general de la LAE y del Real Decreto, pero con registros propios y abriendo más la admisibilidad de otros sistemas de identificación, observando su seguridad y proporcionalidad cuya aplicación habrá que seguir en la práctica.

Por su parte, el artículo 15.2 dispone que "La firma electrónica deberá cumplir las normas establecidas en el protocolo de identificación y firma electrónicas."

Dicho protocolo deberá ser aprobado, entre otros, en el plazo de un año por el titular de la consellería con competencias en materia de administraciones públicas, según se recoge en la Disposición Final Primera del Decreto de la Xunta. Por tanto, este Decreto será desarrollado en este punto antes de diciembre de 2011.

4.5. Seguridad e interoperabilidad: los "esquemas"

Sin duda, otro desarrollo normativo de enorme importancia en el ámbito de la administración electrónica y, en concreto, de la LAE, lo suponen los llamados "esquemas" aprobados por 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, y 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.

Ambos reglamentos abordan dos aspectos fundamentales y no siempre tomados en cuanta en los proyectos de administración electrónica en el pasado: la seguridad y, muy especialmente, la interoperabilidad.

El primero de ellos, sin duda, es obvio: habida cuenta de la ingente y sensible cantidad de información que atesora la administración y que será fácilmente accesible y (por qué no decirlo) manipulable una vez se digitalice mediante sistemas informáticos, se hace necesario establecer un estricto régimen de medidas de seguridad a aplicar a toda la documentación pública electrónica. Esto es lo que realiza el Real Decreto 3/2010 mediante la adopción del llamado "Esquema Nacional de Seguridad" (o "ENS").

Tal y como dispone la Exposición de motivos de dicho Real Decreto:

"La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan."

Bien es cierto que en nuestro Derecho ya contábamos con una herramienta de enorme utilidad a este respecto: el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal dispone en su Título VIII un completo régimen de medidas de seguridad que deben ser adoptadas en todo sistema donde se traten datos de carácter personal (ya sea electrónico o en papel). Sin embargo, esta normativa resulta solamente aplicable a datos personales y no sería aplicable a otra documentación de las

administraciones que no afecten a la privacidad de los ciudadanos.

Así, con el ENS se asegura un régimen más amplio y adaptado aplicable a toda la documentación, datos y archivos obrantes en las Administraciones públicas. Su artículo 1.2 dispone que el ENS "está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias".

Por su parte, el artículo 4 fija los siguientes principios básicos del ENS y que se desarrollan a lo largo de todo su articulado:

Seguridad integral

Gestión de riesgos

Prevención, reacción y recuperación

Líneas de defensa

Reevaluación periódica

Función diferenciada

En lo referente a la firma electrónica, el artículo 33 del ENS se remite a su Anexo II en lo relativo a las medidas de seguridad aplicables. Por su parte, el apartado 2 del mismo dispone 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".

Por tanto, se estará a lo dispuesto en la mencionada política específica a efectos de garantizar la correcta emisión, validación, conservación y uso de las firmas electrónicas dentro de la administración, habida cuenta de lo que supondría un sistema inseguro a este respecto prestándose eventuales errores, suplantaciones e inconsistencias de un sistema documental público que debería ser robusto a fin de garantizar su plena eficacia jurídica.

La interoperabilidad, sin embargo, es, si cabe, tan o más necesaria que la seguridad puesto que es la gran asignatura pendiente de la Administración electrónica hasta la legislación actual: nos referimos a la necesidad de que los datos de todas las administraciones puedan cruzarse e interrelacionarse con los obrantes en otras entidades, siempre de acuerdo con la Ley, sin crear "reinos de Taifas" o sistemas aislados que son incapaces de comunicarse o, si lo hacen, es con grandes dificultades y demoras injustificadas. Por otro lado, los sistemas públicos no deben discriminar a los ciudadanos en función de su elección tec-

nológica, debiendo ser ampliamente compatibles con todas las plataformas informáticas del mercado. Su régimen se desarrolla en el Real Decreto 4/2010 que regula el llamado "Esquema Nacional de Interoperabilidad" (o "ENI").

Su Exposición de Motivos afirma que "la finalidad del Esquema Nacional de Interoperabilidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia".

Así, su artículo 1.2 dispone que el ENI "comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica".

Tal y como lo hacía el ENS, el artículo 4 del ENI establece los siguientes principios básicos que guían la regulación de la interoperabilidad:

La interoperabilidad como cualidad integral.

Carácter multidimensional de la interoperabilidad.

Enfoque de soluciones multilaterales.

En lo referente a la interoperabilidad de firma electrónica y de certificados, el artículo 18 del ENI dispone lo siguiente:

"1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. No obstante, dicha política podrá ser utilizada como referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales. (…)

5. La política de firma electrónica y de certificados, mencionada en el apartado primero del presente artículo, 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. La lista que establezca la Administración General del Estado podrá ser utilizada como re-

ferencia por otras Administraciones públicas para definir sus listas de servicios de confianza para aplicación dentro de sus ámbitos competenciales."

En este sentido, se pretende garantizar el establecimiento de criterios comunes de reconocimiento e interoperabilidad de los distintos sistemas de firma electrónica utilizados y aceptados en el seno de las administraciones públicas: tanto por parte de los ciudadanos y entidades como por las propias administraciones y organismos.

5.

LA FIRMA ELECTRÓNICA EN CIFRAS

A continuación se hace un breve análisis de algunos indicadores relacionados con la certificación digital y la firma electrónica y se dan algunas pinceladas sobre la relación de estos indicadores con el contexto tecnológico existente en la actualidad en España y Galicia.

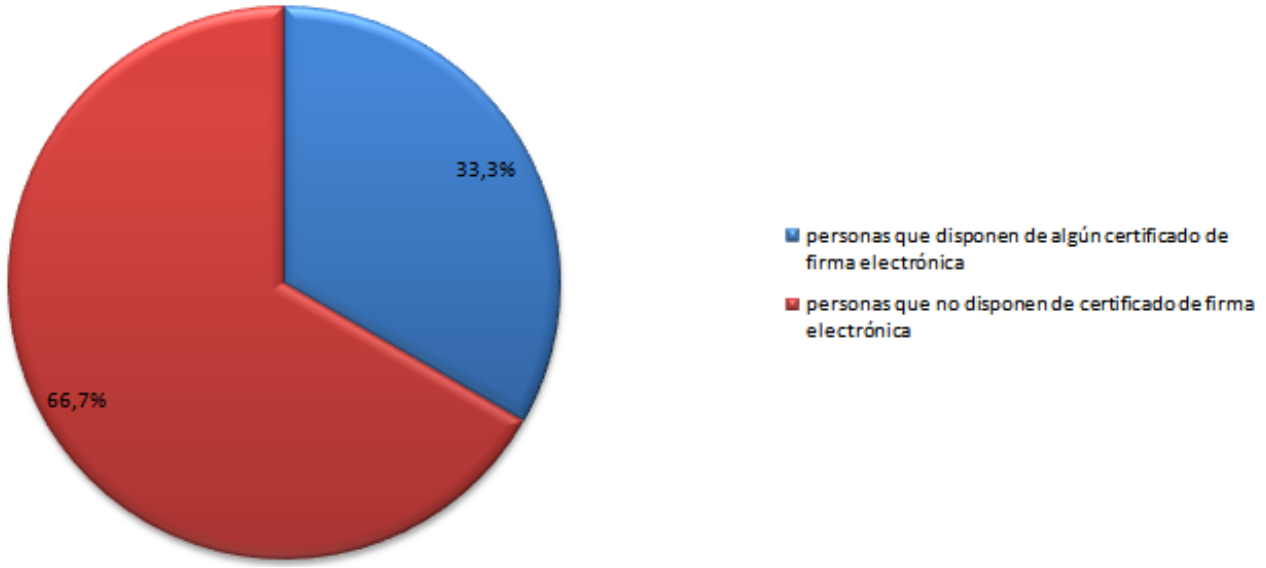
Para el desarrollo de este apartado se han utilizado como fuentes datos procedentes tanto del Instituto Nacional de Estadística como del *Observatorio da Sociedade da Información e a Modernización de Galicia* y hay que tener en cuenta que los datos incluidos en el mismo, siempre que no se indique lo contrario, se refieren al mes de enero del año referido.

CIUDADANOS

En la actualidad **de los 34,6 millones de personas residentes en España, de entre 16 y 74 años, aproximadamente el 27,5% dispone ya de DNI electrónico y sólo el 9% dispone de otros tipos de certificados de firma electrónica reconocidos**.

Algo más de 11,5 millones de personas, es decir aproximadamente un 33% de la población, disponen actualmente de algún certificado de firma electrónica. Esto supone que actualmente en España algo más de 23 millones de personas no tienen ningún tipo de certificado de firma electrónica reconocido.

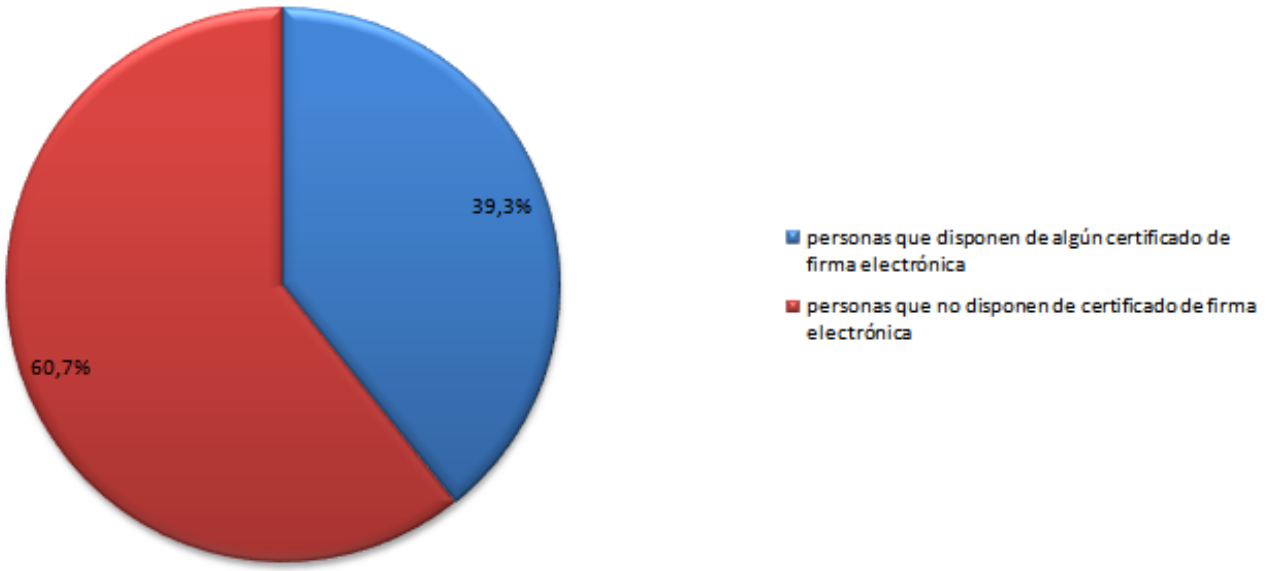
Cabe destacar que hay aproximadamente 100.000 personas de nacionalidades extranjeras residentes en España que disponen actualmente de certificados de firma electrónica reconocidos.



Gráfica 1: Disponibilidad de algún certificado de firma electrónica en España. Año 2010.

BASE: personas residentes en España de entre 16 y 74 años.

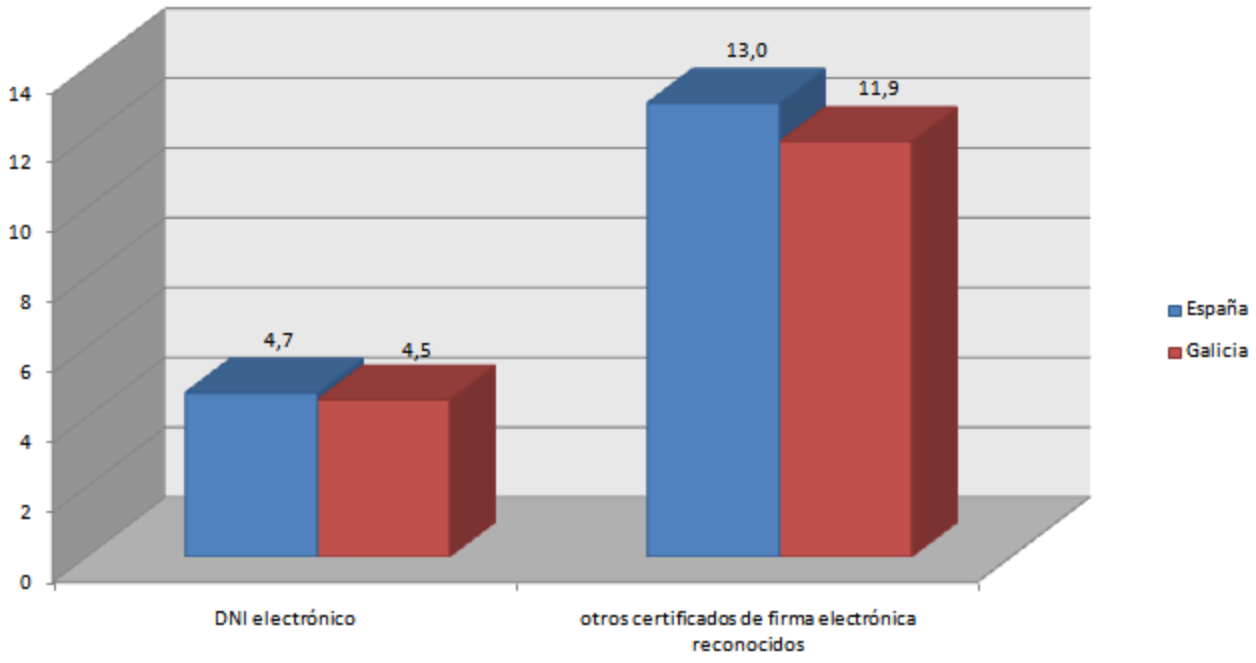
En Galicia, el porcentaje de personas que disponen de algún certificado de firma electrónica es superior a la media de España, y se sitúa algo por encima del 39% de la población (aproximadamente 800.000 personas).



Gráfica 2: Disponibilidad de algún certificado de firma electrónica en Galicia. Año 2010.

BASE: personas residentes en Galicia de entre 16 y 74 años.

Un 4,7% de las personas residentes en España de entre 16 y 74 años han utilizado el DNI electrónico durante el último año para sus relaciones con las Administraciones públicas y el 13% ha utilizado otros certificados de firma reconocidos. Como puede verse en la siguiente gráfica, en Galicia estos datos de utilización son ligeramente inferiores, tanto en el caso del DNI electrónico como en el caso de otros certificados de firma electrónica reconocidos.



Gráfica 3: Utilización de certificados de firma electrónica para las relaciones con las Administraciones Públicas, en Galicia y España. Año 2010.

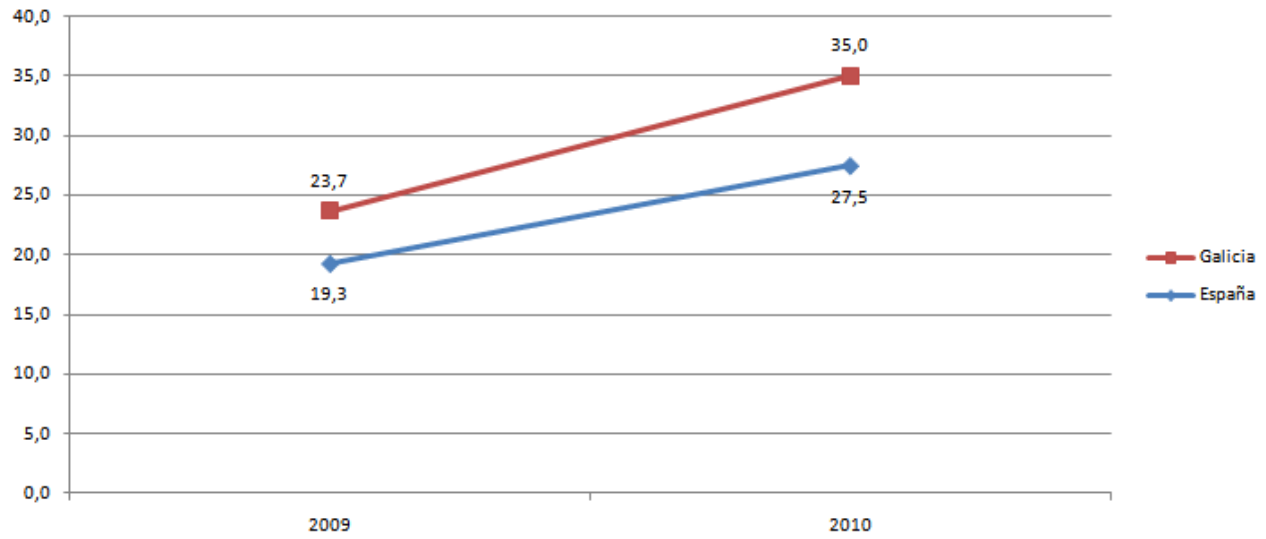
BASE: personas residentes en Galicia y España de entre 16 y 74 años.

De los datos anteriores se concluye que, en general, si bien el DNI electrónico es, con diferencia, el dispositivo de firma electrónica más extendido entre los ciudadanos, no es demasiado utilizado.

Cabe destacar, sin embargo, que existe un segmento de población, el formado por las personas que todavía están realizando estudios, en el que para la relación con las Administración Públicas se ha utilizado más el DNI electrónico que cualquier otro dispositivo.

Es significativo destacar en este punto el dato relativo a la **disponibilidad del DNI electrónico en Galicia** que, con un porcentaje del 35% de la población, es actualmente muy superior a la media en España (7,5 puntos porcentuales más).

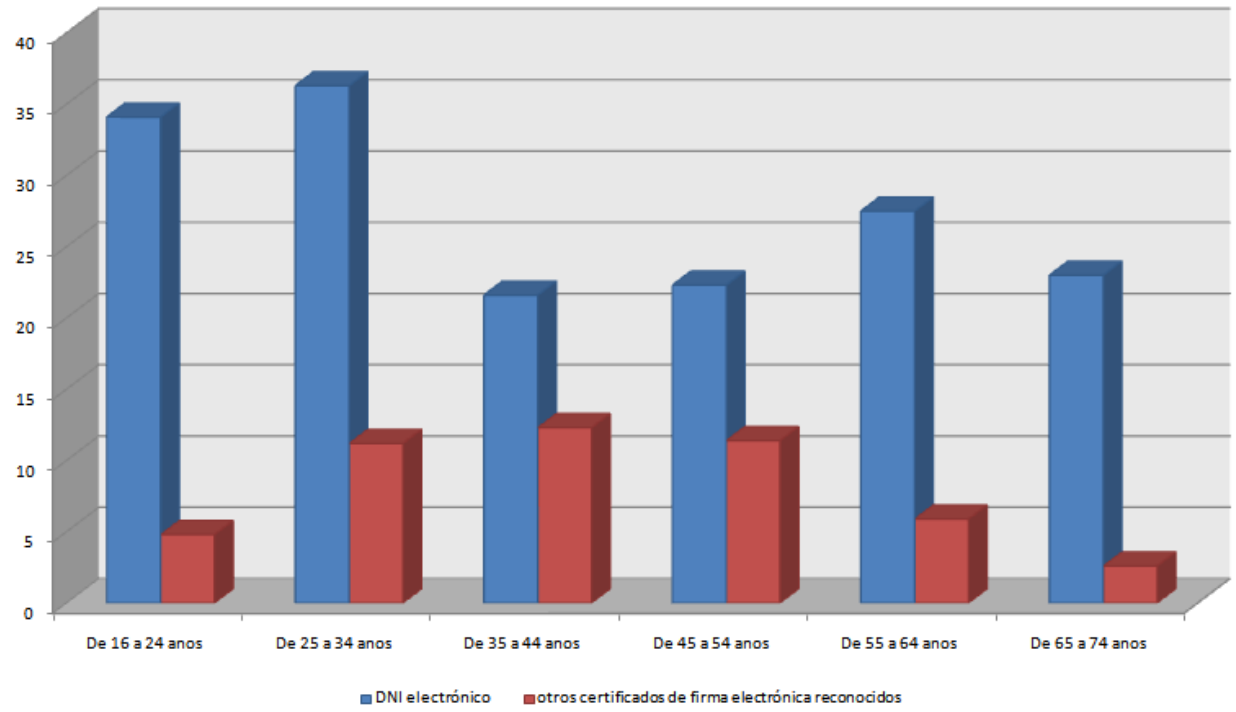
Hay que destacar también, en este sentido, que el incremento en Galicia de la disponibilidad del DNI electrónico se ha situado durante el último año en torno al 48%, pasando del 23,7% en el año 2009 al 35% en el año 2010.



Gráfica 4: Evolución de la disponibilidad del DNI electrónico en Galicia y España. Años 2009-2010.

BASE: total de personas residentes en Galicia y España de entre 16 y 74 años.

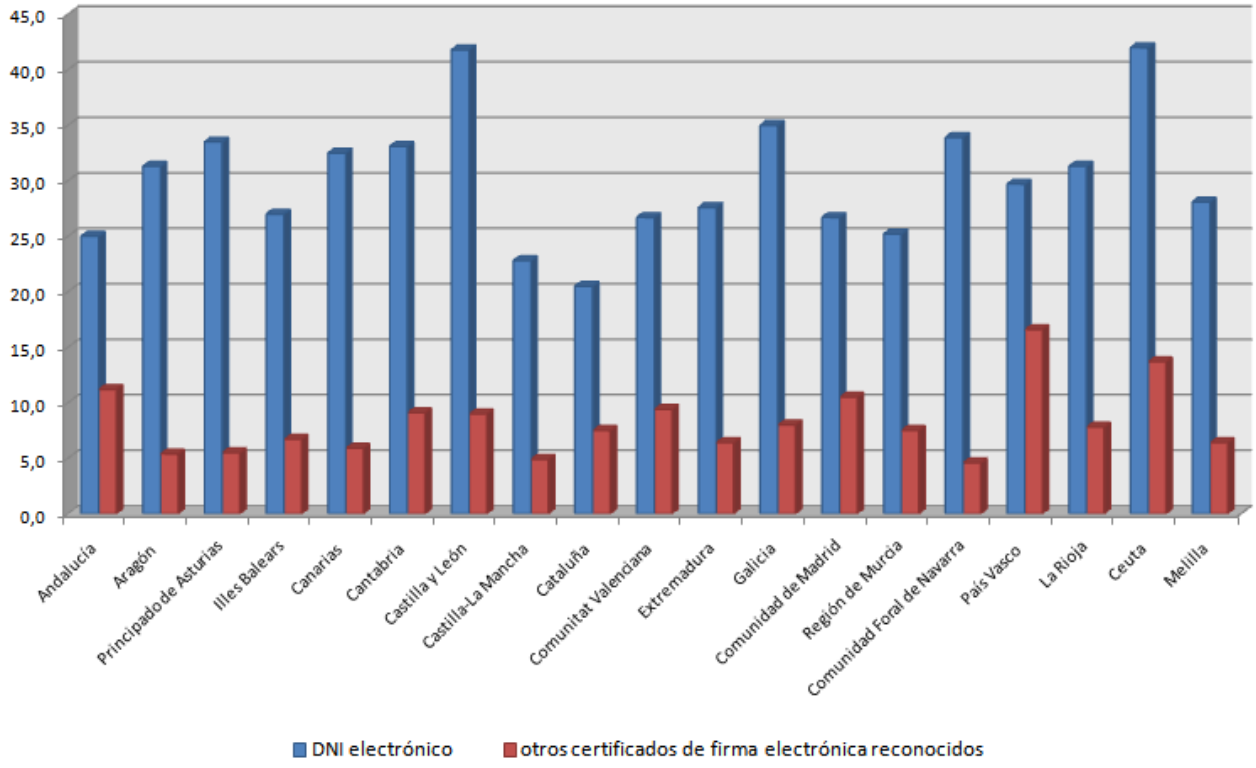
En la siguiente figura se muestra, de manera agrupada por rango de edad, la disposición de DNI electrónico y de otro tipo de certificados por parte de los ciudadanos:



Gráfica 5: Disponibilidad de certificados de firma electrónica (DNI electrónico y otros)

BASE: total de personas residentes en España de entre 16 y 74 años.

Por comunidades autónomas, como puede apreciarse en la siguiente tabla, la disponibilidad del DNI electrónico varía entre casi el 42% de Castilla y León y Ceuta y el escaso 20% de Cataluña. En el caso de otros certificados de firma electrónica reconocidos la disponibilidad varía entre el 16,6% en el País Vasco y el 4,6% de la Comunidad Foral de Navarra.



Gráfica 6: Disponibilidad de certificados de firma electrónica (DNI electrónico y otros)

BASE: total de personas residentes en España de entre 16 y 74 años.

Resulta sorprendente, a la vista de los datos anteriores, que Comunidades Autónomas con entidad de certificación propia, como Cataluña o la Comunidad Valencia, no despunten de manera destacada sobre el resto de Comunidades Autónomas en cuanto a la disponibilidad de certificados de firma electrónica reconocidos de sus ciudadanos. Sin embargo, la disponibilidad de certificados de firma electrónica, diferente al DNI electrónico, en el País Vasco (otra de las comunidades con entidad de certificación) si es significativamente mayor que la media.

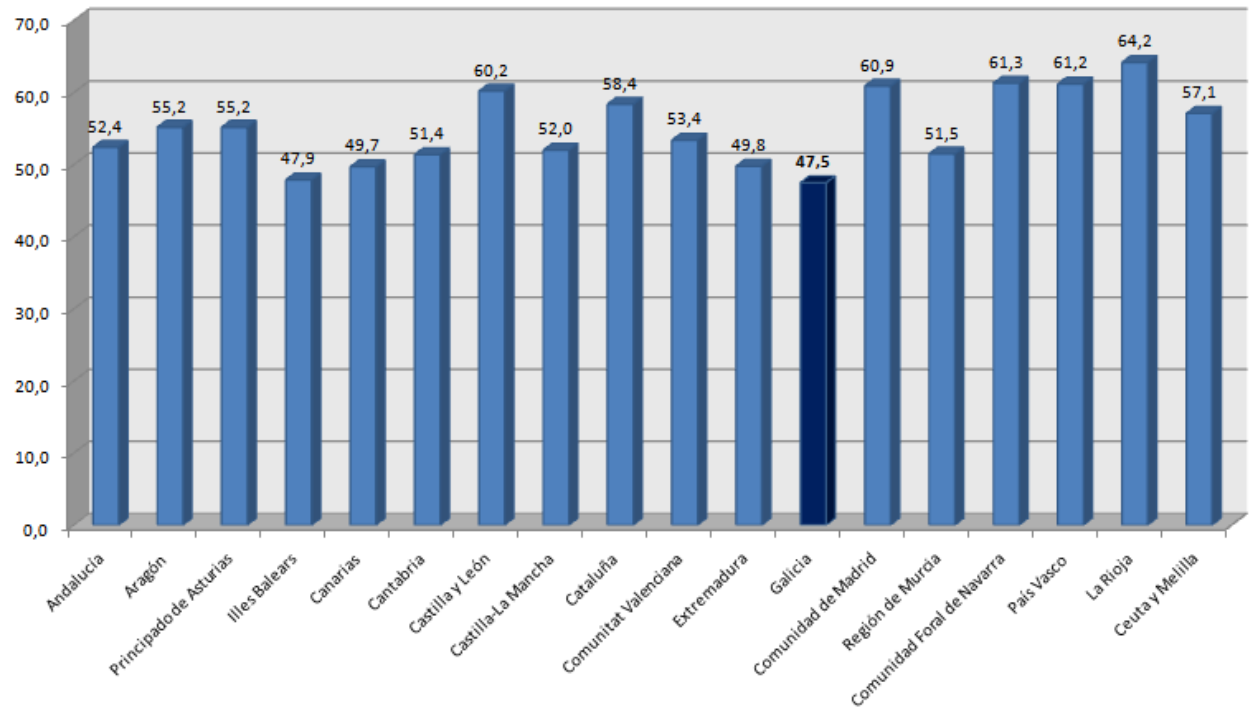
A continuación se detallan algunos datos significativos que ayudan a contextualizar el entorno tecnológico actual de la población de Galicia y España:

INDICADORES TECNOLÓGICOS	2008		2009		2010	
	España	Galicia	España	Galicia	España	Galicia
Viviendas con algún tipo de ordenador	63,6%	53,6%	66,3%	58,5%	68,7%	61,6%
Viviendas que disponen de acceso a Internet	51,0%	39,7%	54,0%	42,3%	59,1%	48,9%
Viviendas con conexión de banda larga (ADSL, cable,…)	44,6%	31,8%	51,3%	38,3%	57,4%	46,5%
Porcentaje de Viviendas con teléfono fijo	81,3%	81,8%	80,3%	80,7%	80,3%	78,5%
Porcentaje de Viviendas con teléfono móvil	92,1%	87,0%	93,5%	89,8%	94,6%	91,6%

EMPRESAS DE 10 Y MÁS EMPLEADOS

En España **el 55,7% de las empresas en España de 10 y más empleados con conexión a Internet, utilizó firma electrónica en alguna comunicación enviada durante el último año** desde su empresa.

Este dato de la utilización de la firma electrónica para comunicaciones enviadas por empresas de 10 o más empleados, desglosado por Comunidad Autónoma, se muestra en el siguiente gráfico:

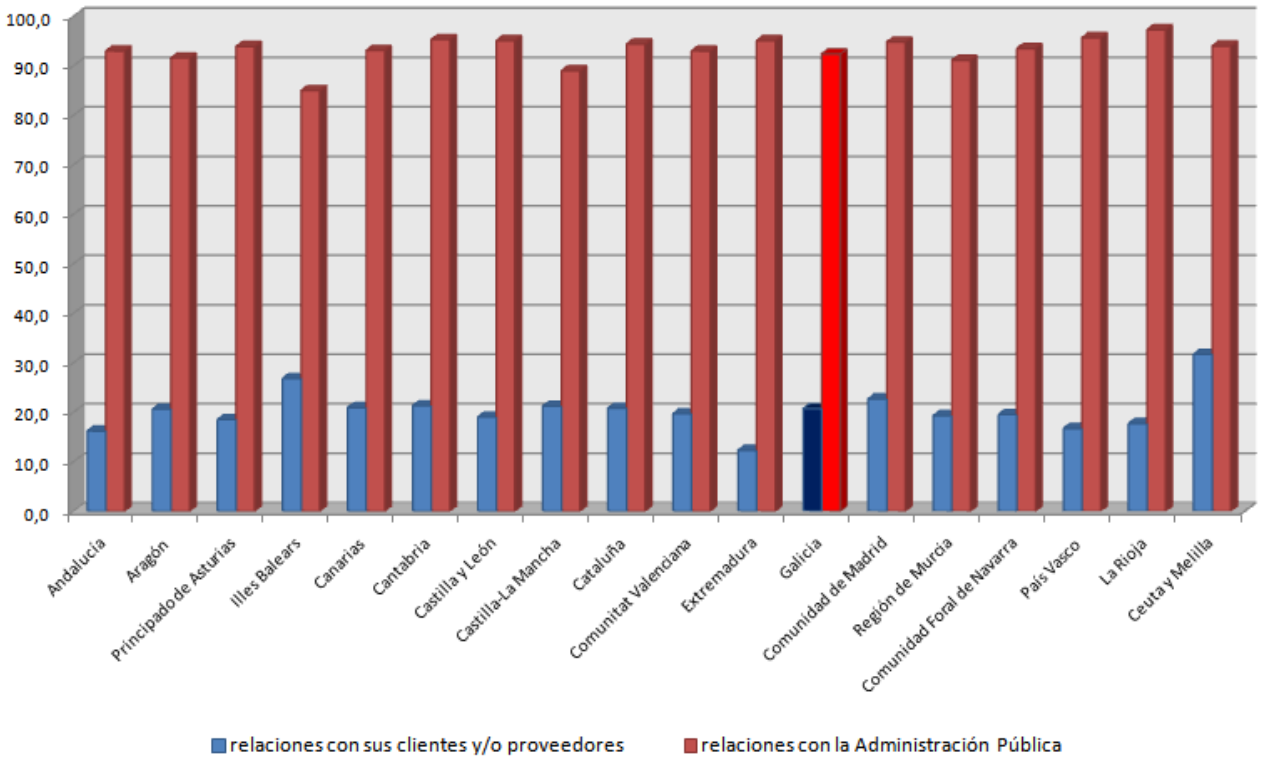


Gráfica 7: Utilización de firma electrónica en alguna comunicación enviada durante el último año

BASE: empresas de 10 y más empleados con conexión a Internet. Año 2010.

Como puede apreciarse en el gráfico, el grado de utilización de la firma electrónica por parte de las empresas varía sustancialmente entre las diferentes comunidades autónomas y se sitúa entre el 64,2% de La Rioja y el 47,5% de Galicia, que en este aspecto se sitúa muy por debajo de la media en España.

Prácticamente la totalidad de las empresas (93,5%), que utilizaron firma electrónica en alguna comunicación enviada durante el último año, la utilizó para relacionarse con la Administración Pública mientras que sólo un 20% lo hizo para relacionarse con sus clientes y/o proveedores.

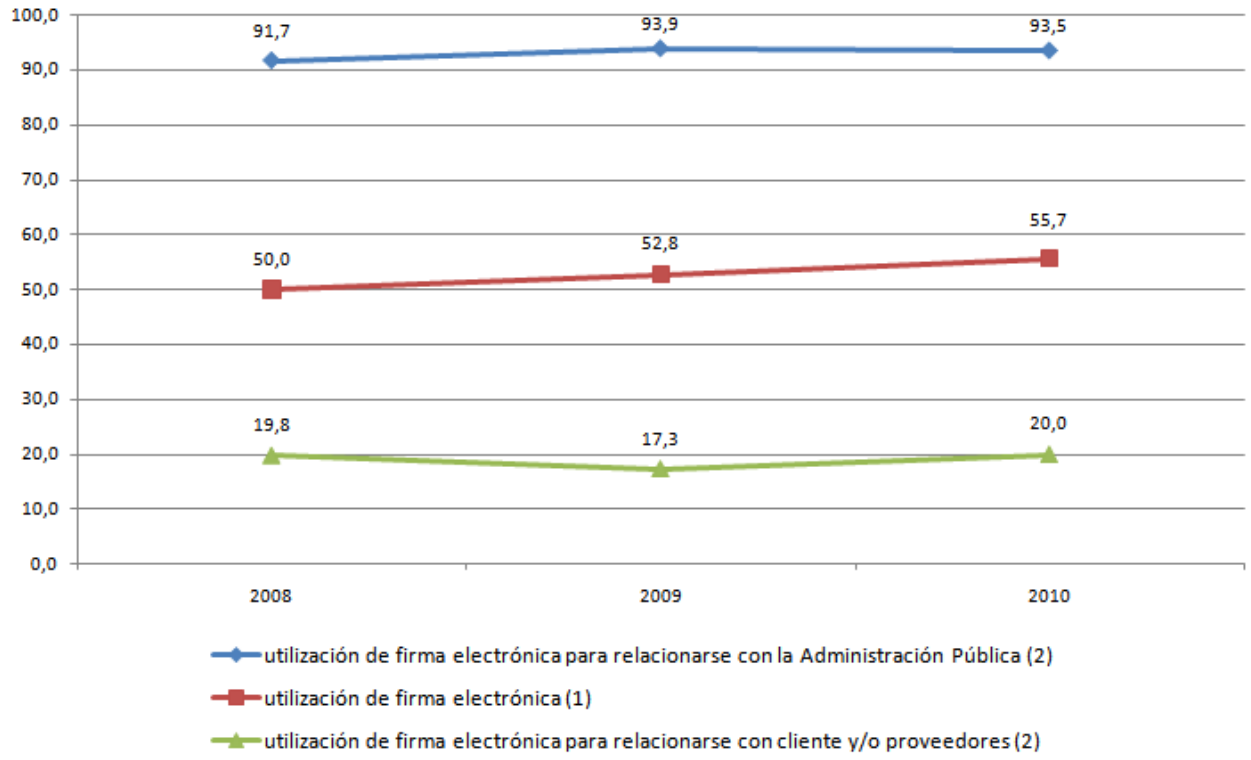


Gráfica 8: Utilización de firma electrónica en alguna comunicación enviada durante el último año

BASE: empresas de 10 y más empleados con conexión a Internet que utilizó firma electrónica en alguna comunicación enviada. Año 2010.

Como puede apreciarse en todas las Comunidades Autónomas, sin excepción, la utilización de la firma electrónica por parte de las empresas para las relaciones con las Administraciones Públicas es significativamente mayor que para las relaciones con sus clientes y proveedores.

Como puede observarse en el gráfico siguiente **en los últimos años se ha producido un avance moderado en la utilización por parte de las empresas de la firma electrónica**.



Gráfica 9: Evolución de la utilización por parte de las empresas de la firma electrónica

BASE (1): empresas de 10 y más empleados con conexión a Internet. Año 2010.

BASE (2): empresas de 10 y más empleados con conexión a Internet que utilizó firma electrónica en alguna comunicación enviada. Año 2010.

A continuación se detallan algunos datos significativos que ayudan a contextualizar el entorno tecnológico actual existente en Galicia y en el conjunto del estado:

INDICADORES TECNOLÓGICOS	2009		2010	
	España	Galicia	España	Galicia
Empresas con ordenador	98,6%	97,1%	98,6%	98%
Empresas con conexión a Internet	96,2%	92,9%	97,2%	94,9%

INDICADORES TECNOLÓGICOS	2009		2010	
	España	Galicia	España	Galicia
Empresas con correo electrónico	94,7%	90,6%	96,5%	94,5%
Porcentaje de empresas que realizaron intercambio electrónico de datos entre empresas	36,7%	33,6%	45,0%	39,6%
Porcentaje de empresas que realizaron intercambio electrónico de datos mediante envío de pedidos a sus proveedores [1]	21,5%	20,3%	51,2%	56,3%
Porcentaje de empresas que realizaron intercambio electrónico de datos mediante recepción de facturas electrónicas [1]	41,0%	26%	51,2%	58,8%
Porcentaje de empresas que realizaron intercambio electrónico de datos mediante recepción de pedidos de clientes [1]	17,0%	17,2%	19,3%	17,8%
Porcentaje de empresas que realizaron intercambio electrónico de datos mediante envío de facturas electrónicas [1]	23,1%	19,2%	25,1%	22,8%
Porcentaje de empresas que realizaron intercambio electrónico de datos mediante envío o recepción de información sobre productos [1]	57,4%	61%	63,1%	63,9%
Porcentaje de empresas que realizaron intercambio electrónico de datos mediante envío o recepción de documentación sobre transporte, envíos o entregas [1]	42,9%	44,5%	50,5%	53,6%
Porcentaje de empresas que realizaron intercambio electrónico de datos mediante envío de instrucciones de pago a entidades bancarias [1]	75,5%	72,9%	74%	71,5%
Porcentaje de empresas que realizaron intercambio electrónico de datos mediante intercambio automatizado de información con la AAPP [1]	60,0%	59,9%	56,6%	57,5%
Porcentaje de empresas que compartían electrónicamente información con sus proveedores o clientes de la cadena de suministro	14,2%	13,7%	17,6%	15%

[1] Porcentaje sobre el total de empresas que realiza intercambio electrónico de datos

6.

LOS RETOS DEL FUTURO EN LA IDENTIDAD DIGITAL

DIVULGACIÓN, FORMACIÓN Y USABILIDAD

En los últimos años se están llevando a cabo labores de divulgación y formación sobre los beneficios y utilización de los certificados electrónicos.

El Ministerio de Industria, Turismo y Comercio trata de fomentar el uso del DNIe impartiendo sesiones formativas presenciales, donde se aborda una parte teórica que se complementa con una sesión formativa on-line. Estas sesiones son gratuitas y basta con inscribirse previamente a través de un formulario web en www.formaciondni.es. En estas jornadas tiene especial importancia transmitir al ciudadano los procedimientos de manera sencilla y clara.

La Administración Pública debe asumir el reto de la mejora continua para la implantación del DNIe, y mirar hacia otros países donde la emisión del certificado electrónico de ciudadano es acompañada por servicios de formación, ayuda e incluso provisión de un lector de cara a facilitar y promover su uso desde el momento de la emisión.

Por otra parte, esta labor de formación, divulgación y asesoramiento se está llevando a cabo también en el ámbito empresarial, en gran parte por los prestadores de servicios de certificación electrónica. Contar con una estrategia de apoyo clara por parte de la Administración Pública será importantísimo para potenciar este reto de transmitir los beneficios y ahorro de costes que aporta a las organizaciones la utilización de la certificación electrónica, actualizando como catalizador de dicho proceso. En el actual escenario de crisis cada punto de mejora por pequeño que sea es importante, y la utilización de la firma electrónica de cara a la optimización de procesos puede ser una de las claves para la mejora de la productividad.

Junto a las necesidades anteriormente descritas existe un elemento muy importante: la usabilidad. Podríamos decir que el certificado debería llegar a ser "invisible", entendiendo como tal que su uso debe ser fácil, natural y casi transparente para los ciudadanos. En este reto juegan un papel relevante factores como el dispositivo que contiene el certificado, su compatibilidad, las aplicaciones o los operadores de comunicaciones entre otros, y uno de los retos es que tendrán que trabajar de manera coordinada en el futuro para alcanzar dichos objetivos.

El hecho de que seamos capaces de convertir a los ciudadanos en e-ciudadanos dependerá en buena medida de que la administración electrónica sea una realidad y que las empresas ofrezcan sus servicios en la red con las mismas condiciones, garantías y seguridad que en su modelo tradicional.

INTEROPERABILIDAD Y ESTANDARIZACIÓN

En un escenario global de eliminación de barreras tecnológicas y físicas no se entiende

el uso de sistemas aislados, que trabajen de manera autónoma. La certificación electrónica no puede ser una excepción y se debe prestar especial importancia a que todos los dispositivos y sistemas sean interoperables y se basen en la utilización de estándares. Esto nos permitirá por una parte mantener la neutralidad tecnológica y por otra abrir nuestras fronteras electrónicas a Europa en un principio y al resto del mundo después.

Desde un punto de vista técnico la convergencia tecnológica de dispositivos facilitará esta labor, y paralelo a ello los sistemas de información evolucionarán hacia la utilización de formatos abiertos como XML o XADES-XL, permitiendo la correcta identificación y codificación de campos y atributos, y hacia la compatibilidad sintáctica o semántica con la utilización de repositorios sincronizados, dotando todo ello a las soluciones de un gran valor añadido.

España debe estar interesada en conseguir esta interoperabilidad cuanto antes, sobre todo teniendo en cuenta el papel de liderazgo que en este sector ocupa España y las posibilidades de negocio que se abren fuera de nuestras fronteras, sobre todo con los países latinoamericanos.

En un escenario a largo plazo es interesante seguir la evolución del proyecto STORK que permitirá conseguir el reconocimiento paneuropeo de las identidades electrónicas, y en concreto la aceptación del DNI electrónico e identificadores similares en servicios de Administración electrónica de otros Administraciones europea.

RETOS LEGISLATIVOS

El principal reto al que se enfrenta nuestra legislación es la plena adaptación de la misma a los nuevos medios digitales, sin poner trabas o requisitos formales innecesarios para la generalización y plenos reconocimiento de los documentos digitales en la totalidad del tráfico jurídico, tanto en el ámbito público como en el privado.

La proverbial (y, a veces, necesaria) lentitud del Derecho a la hora de adaptarse y regular las nuevas realidades, se convierte en un verdadero lastre en el vertiginoso mundo tecnológico de hoy en día. La nueva Sociedad digital demanda soluciones ágiles y dinámicas que aporten seguridad jurídica a los millones de transacciones que se dan todos los días en Internet.

Nuestra capacidad productiva y competitiva depende de ello en este nuevo escenario tan cambiante y globalizado.

El vértigo que podamos sentir ante el desconocimiento de las nuevas tecnologías y la inseguridad que instintivamente sentimos ante lo que no podemos tocar y oler, no debe hacernos caer en imponer más exigencias al mundo virtual de las que ya aplicamos en el

mundo físico. Desgraciadamente, mucha de nuestra normativa actual es muestra patente de ello como, por ejemplo, nuestra actual regulación de la factura electrónica cuyos requisitos superan con mucho los aplicables a la factura en papel y todavía mucho más a los que se piden en la práctica respecto a estas últimas. En nuestra opinión, dicha legislación debe aligerarse y flexibilizarse sin perder nunca de vista los criterios y principios de interoperabilidad y de neutralidad tecnológica que hemos comentado anteriormente.

Es posible lograr una seguridad jurídica suficiente en el mundo digital sin poner trabas innecesarias y/o excesivas a los sujetos que deciden utilizarlo como principal o, incluso, único medio de operar en el mercado y en la sociedad actual.

El futuro, sin duda, nos lo demanda.

SEGURIDAD

El incremento en el uso de las comunicaciones a través de internet tanto en las relaciones personales como en las comerciales conlleva unos riesgos que se deben minimizar. De hecho la inseguridad es uno de las grandes barreras a la utilización profesional y comercial de internet, y con el impulso que están tomando las redes sociales podría serlo también a nivel personal.

La utilización de elementos como el certificado electrónico personal o profesional, el certificado de sede electrónica, o cualquier mecanismo que garantice que la entidad o la persona que está al otro lado es quien dice ser y además es segura, promueven y fortalecen la utilización de transacciones comerciales a través de la red. En este proceso confluyen múltiples actores, desde el fabricante de los dispositivos que albergan el certificado, las autoridades de certificación que llevan a cabo la validación y los proveedores de servicio o fabricantes de software, sin olvidarnos del papel que ocupa la Justicia en la definición de un marco legal en continua adaptación que regula la participación de dichas entidades.

Es importante destacar que en el ámbito de seguridad el certificado electrónico no es un mecanismo o solución exclusiva sino que aporta un valor añadido importantísimo en entornos que lo complementan con otros elementos, por ejemplo biométricos, para dotar a las soluciones de los más exigentes niveles de seguridad.

En el ámbito de la seguridad el INTECO ha desarrollado una iniciativa muy interesante para ofrecer a la industria un esquema de certificación contra una norma nacional e internacional de requisitos de seguridad que permitiera que las aplicaciones y servicios que se certifiquen contra dichos perfiles dispusieran de mayores garantías de seguridad y confianza. Las aplicaciones que se desarrollen apoyándose en estos perfiles pueden por un lado disponer de mejores requisitos de seguridad, y por otro lado llevar a cabo un proceso

formal de evaluación y certificación contra dichos perfiles, obteniendo un certificado de nivel Common Criteria que les aporte también un sello de calidad y una herramienta más de competitividad. Asimismo otras aplicaciones o servicios que se apoyen en firma electrónica o digital pueden también seguir procesos de certificación similares y elevar su nivel de seguridad así como su imagen hacia el exterior ganando confianza en el sector que va a usar dichas aplicaciones.

CONVIVENCIA DE ENTIDADES PÚBLICAS Y PRIVADAS

La oferta y demanda funcionan habitualmente como regulador de los mercados, pero se necesitan una serie de normas que sean de obligado cumplimiento y cuya aplicación evite conflictos de intereses que impidan o retrasen la evolución de las certificaciones electrónicas en un mercado global.

Cuando el DNIe despegue ocupará posiblemente el hueco de certificado de ciudadano y desplazará al de otras entidades, con lo que podríamos decir que a largo plazo tendría sentido que desaparecieran las iniciativas públicas o privadas de expedir identidades digitales personales. El DNIe es un servicio capaz de gestionar la mayor parte de las necesidades de identificación a nivel personal y curiosamente el sector privado no lo ve como una amenaza, sino como un habilitador o dinamizador del proceso.

Sin embargo a nivel empresarial el certificado de profesional cubrirá las necesidades de los profesionales, asociados o empresas para las que no sirve el DNIe. Ahí es donde se centrará con total seguridad el desarrollo del negocio de las entidades de certificación privadas, e incluso el de la FNMT. Si garantizamos el cumplimiento de la legislación que establece las obligaciones y responsabilidades de los prestadores de servicios de certificación y su propia certificación, deberían poder convivir ambos tipos de entidades de manera armónica y velando por unos intereses comunes.

FACTURACIÓN Y ADMINISTRACIÓN ELECTRÓNICA

Si hablamos de sistemas de información y certificación electrónica existen dos puntos de encuentro que no podemos excusar, se trata de la facturación electrónica y de la contratación electrónica en Administración Pública. Quizás veamos lejos un nivel alto en la implantación y consolidación de estas tecnologías, pero desde luego será un salto cualitativo muy importante de cara a mejorar la productividad en España.

El sector industria demanda una facturación electrónica integrada con los sistemas de información de los canales de producción, almacenamiento y logística, que permita en tiempo real tener el control de su negocio. Este cambio gradual conllevaría un ahorro de

costes de almacenamiento y seguramente la orientación de las empresas de fabricación a la utilización de metodologías y procesos de producción "just in time" con las consiguientes ventajas de productividad de la que ya hemos hablado.

Por otra parte los procesos de la Administración Pública podrían orientarse a flujos de trabajo integrados desde el inicio hasta el fin con los ciudadanos y las empresas, y que les permitan garantizar la integridad, transparencia y seguridad de sus procedimientos. Por otra parte la calidad del servicio percibido por los usuarios se incrementaría considerablemente puesto que permitiría la igualdad de servicios independientemente del lugar de residencia o la alta disponibilidad de los servicios de Administración Pública las veinticuatro horas del día y los siete días de la semana.

Este reto podría aplicarse a otros sistemas de información relacionados con la certificación electrónica, y cuyo objetivo común con los dos que detallamos será siempre la optimización y mejora de procesos tanto productivos como organizativos.

7. CONCLUSIONES

CERTIFICADOS DIGITALES

La certificación electrónica es fundamentalmente un tema de **confianza y seguridad**. La certificación electrónica permite **realizar a través de Internet todo tipo de trámites de manera segura** garantizando la verdadera identidad del usuario y permite la firma electrónica de documentos con la misma validez legal que si se firmaran de puño y letra en papel. La tramitación online permite a los usuarios realizar multitud de gestiones durante 24 horas al día, evitando desplazamientos y esperas y generando ahorro de tiempo, intermediarios, errores, archivo físico y gastos de transporte.

Actualmente los ciudadanos que utilizan la firma electrónica tienen claro su valor de seguridad pero, en general, los ciudadanos todavía no perciben con claridad su utilidad ni su eficacia. Uno de los principales motivos del poco uso de la firma electrónica y del certificado digital se debe al desconocimiento que hay de sus posibilidades y garantías, tanto a nivel empresarial como en la ciudadanía.

Hay que tener en cuenta, además, que la conocida como alfabetización digital es todavía escasa entre la población, y las dificultades de comprensión de estas tecnologías y el estado todavía incipiente de la "vida digital" hacen necesaria una optimización de las aplicaciones de cara a un uso amigable y compatible con todos los sistemas. Se debe conseguir que el uso de los certificados digitales sea tan fácil y transparente que se haga invisible para el ciudadano.

La **estrategia de despliegue de los certificados electrónicos** debe estar en función de los proyectos que surjan y de la propia demanda, es decir, no se deben crear necesidades artificiales de certificados electrónicos sino adaptar éstos a la demanda y a las necesidades reales existentes. Hay que hacer un planteamiento adecuado de para qué vale la certificación digital y la firma electrónica y en qué ámbitos tiene sentido su utilización, poniendo por delante del despliegue de certificados y tarjetas el desarrollo de los sistemas de información que los necesitan. Será el propio mercado y los usuarios los que marcarán la tendencia en todas las soluciones y los retos futuros.

UTILIZACIÓN DE LOS CERTIFICADOS DIGITALES

Actualmente la utilización de la certificación electrónica en España está, con diferencia, **más extendida en la Administración Pública que en la empresa privada**, siendo la Agencia Tributaria el organismo referente hasta el momento por el uso de los certificados para la realización de la Declaración de la Renta.

Existe una diferencia muy importante entre Europa y España en el uso del certificado digital ya que, mientras que en Europa el motor de promoción de esta tecnología ha sido

la empresa privada (fundamentalmente la banca), en España ha sido la Administración Pública , en especial como se ha comentado, la Agencia Tributaria y en menor medida las cámaras de comercio y los colegios profesionales.

Dentro de la Administración Pública existen diferentes grados de implantación pero en general, en estos últimos años, se ha desarrollado un esfuerzo muy importante por modernizar y agilizar los trámites telemáticos en la mayoría de Comunidades Autónomas y en muchas Corporaciones Locales. El escenario actual de crisis económica ha supuesto un parón en los avances en esta materia que hubieran sido mayores, cuantitativa y cualitativamente hablando, en una situación económica normal.

Sin duda las empresas privadas siguen un ritmo bastante más lento en la adopción de la firma electrónica que las Administraciones Públicas. Esto puede deberse a que **el retorno de la inversión realizada en materia de certificación electrónica es un retorno "no inmediato"**. Las Administraciones Públicas se mueven por el interés de prestar más y mejores servicios a los ciudadanos y miden el retorno de la inversión en parámetros como seguridad o beneficios sociales. Sin embargo es probable que la percepción de calidad y seguridad de este tipo de sistemas por parte de los usuarios comprometa a las empresas privadas, que quieren cuidar su imagen, a ofrecer servicios más seguros a través de Internet utilizando este tipo de certificados.

Cuando la Administración Pública termine de implantar todos sus sistemas, sus sedes electrónicas, factura electrónica,… será el momento en que se obligue a sus proveedores a usar certificados digitales y a los ciudadanos a usar, por ejemplo, el DNIe.

Un paso importante que se debería abordar desde el sector es el ayudar a la empresa privada, a la Administración Pública y la ciudadanía a distinguir sobre la gran variedad de tipos de certificados digitales existentes en la actualidad: con uso limitado a los trámites con las Administraciones Públicas, certificados de atributo para el mundo empresarial para firmar documentos, certificados vinculando al trabajador a una empresa con un cargo determinado en la misma, DNIe,…

DNIe

Es muy destacable, en el panorama actual, la funcionalidad aportada por el DNIe en la certificación digital, como un dispositivo seguro que facilita al ciudadano la realización de trámites con total seguridad. Este **proyecto de identidad digital es pionero en Europa** y ha servido como referencia a otros países que comienzan ahora con proyectos similares, apoyándose en el conocimiento generado por la experiencia española.

La implantación definitiva del DNIe supondrá, a medio o largo plazo, el fin de los certifica-

dos de ciudadano que la mayoría de los proveedores de servicios de certificación emiten actualmente.

El DNIe será una **gran ayuda de cara al ciudadano aunque es evidente que necesita mejorar su usabilidad**. El DNIe tiene el inconveniente, que supone una barrera que todavía hay que superar, de necesitar un lector del que no todos los ordenadores disponen. Esta razón, junto con la escasa información que se ha ofrecido a la ciudadanía sobre su uso, es uno de los principales aspectos por los que hoy en día no todo el mundo tiene acceso o conocimiento para realizar operaciones con el DNIe.

UNIFICACIÓN DE DISPOSITIVOS

El futuro de la certificación digital pasa, entre otras cosas, por unificar dispositivos y definir usos y funciones. Si realmente se quiere convertir al ciudadano en un ciudadano digital es necesario realizar una convergencia de dispositivos unificando todos los dispositivos en uno sólo, manejable y comprensible.

e-ADMINISTRACIÓN

Los grandes avances tecnológicos que se han producido en los últimos años se ponen, mediante la e-administración, a disposición de la ciudadanía y del día a día de la Administración Pública. La tecnología llega actualmente a todas partes y los propios ciudadanos son cada vez más exigentes para que la propia administración ofrezca servicios telemáticos.

Sin embargo, **los ciudadanos tienen que percibir la e-administración como una realidad que es ventajosa** y que les va a proporcionar mejores relaciones con la administración. Si la administración ofrece servicios importantes para el usuario a través de Internet seguro que el ciudadano va a utilizarlos. Hay que tener en cuenta, además, que actualmente cualquier ciudadano puede exigir que cualquier procedimiento esté en Internet.

Aunque pueda parecer que hoy en día la certificación electrónica se limita a trámites muy concretos hay que tener en cuenta que, como sucedió en otros aspectos, todo proceso nuevo comienza de manera similar y primero se automatizan y modernizan aquellos 4 o 5 trámites que suponen el 80 por ciento de los servicios prestados a los ciudadanos y, posteriormente, se automatizan cientos de ellos que dan lugar al 20 por ciento residual. En estos momentos **la mayoría de Comunidades Autónomas y ayuntamientos grandes y medios se encuentran en una fase de despliegue de la e-administración ya bastante avanzada**, tendiendo a una consolidación de la misma. Por el contrario, son los pequeños ayuntamientos los que se encuentran en una posición más retraída en este sentido.

Hay que tener en cuenta que **la implantación electrónica necesita ir siempre a la par de la implantación de infraestructuras**. En este sentido, muchas Comunidades Autónomas han definido de manera acertada una estrategia de infraestructuras (banda ancha,…) que favorece la implantación de los servicios digitales especialmente en los municipios con mayores dificultades.

Aunque el cumplimiento completo y exhaustivo de la Ley 11/2007 es muy difícil y supone un proceso lento, las comunidades autónomas han avanzado de manera notable en los últimos meses en su adaptación a la misma.

En la actualidad **las barreras a la administración electrónica vienen impuestas por la usabilidad de las propias tecnologías y por el cambio cultural y de hábitos** que esta nueva administración requiere.

INTEROPERABILIDAD

El futuro de la certificación electrónica pasa por la **interoperabilidad real dentro de la Unión Europea**, en un primer nivel, y con el resto de los países en otro segundo nivel, llevando a cabo macroacuerdos entre las entidades. La tendencia es que en un futuro inmediato haya la obligación de que todos los prestadores en el marco europeo se admitan entre ellos, tendiendo progresivamente hacia una conjunción de sistemas tecnológicos e informáticos, logrando un marco europeo de homologación único y, probablemente, creando una autoridad común europea o un órgano intermediario en materia de identificación digital que actúe de enlace entre todos los países y sus entidades de certificación digital.

Actualmente **se está discutiendo sobre cómo liberar las políticas en materia de certificación digital** ya que, todavía ahora, existen certificados con políticas muy restrictivas, lo que provoca que en algunos casos una persona deba disponer obligatoriamente de varios certificados. Esta situación también determina la necesidad de que funcione un organismo de carácter supranacional que realice las validaciones de identidad.

Actualmente, aunque existen diversos proyectos para el uso de la certificación electrónica a nivel europeo e internacional, éstos se están encontrando con graves dificultades de interoperabilidad debido a los diferentes sistemas de uso de los certificados, como las certificaciones cruzadas, en las que es difícil delimitar las responsabilidades entre las partes. Hoy en día todavía no se ha llegado a una solución global en este aspecto.

En este sentido se ha trabajado a nivel europeo en el proyecto STORK, para conseguir el reconocimiento paneuropeo de las identidades electrónicas y a nivel español en la creación de una línea TSL´s, o listas de confianza interoperables entre estados miembros.

Para España, específicamente, es muy importante desde el punto de vista económico, ser

interoperable con países de Latinoamérica, puesto que son vías de negocio para los proveedores de servicio españoles.

PROVEEDORES DE SERVICIOS

El mercado en torno a la certificación digital es todavía incipiente en España a pesar de que nuestro país cuenta ya con un número considerable de prestadores de servicios.

La situación actual del mercado en torno a los proveedores de servicios parece pronosticar la posible desaparición de los pequeños proveedores o el establecimiento de alianzas entre ellos para generar servicios de calidad y de valor añadido, optimizando los recursos. Todos los prestadores de servicios de certificación comparten un espacio común, en el que la competencia y la competitividad son buenas, y será la ley de la oferta y la demanda la que decida **qué proveedores de servicios de certificación continuarán y cuáles desaparecerán**.

A largo plazo parece lógico que únicamente sólo se utilicen los certificados de empleado público y los certificados de atributo o empresariales, que permitirán la supervivencia de las entidades de certificación públicas y privadas y el DNIe.

En España, a la creación de organismos prestadores de servicios de certificación digital a nivel estatal, públicos y privados, se han unido también las iniciativas de las comunidades autónomas que han optado por disponer de autoridades propias, diferentes y adaptadas a su realidad

En principio el hecho de que una Comunidad Autónoma, o incluso una Corporación Local, decida convertirse en entidad de certificación no parece responder a una cuestión de ahorro económico, puesto que es más rentable compartir recursos que desarrollar un servicio propio, ni de compatibilidad o tecnológica.

La **creación de autoridades de certificación propias en las comunidades autónomas** está justificada siempre y cuando éstas tengan una orientación global, emitan documentos que sirvan para realizar tramitaciones en cualquier otra comunidad autónoma y cumplan otra serie de cualidades de valor añadiro. Una Comunidad Autónoma no debe ser sólo un tercero de confianza o un mero validador que da crédito y fe, sino que debe ser la vanguardia de la administración electrónica, ofreciendo servicios de valor añadido a los ciudadanos y fomentando el uso y el desarrollo de la certificación electrónica en la administración con las necesarias garantías de seguridad, confidencialidad, autenticidad e irrevocabilidad de las transacciones.

LEGISLACIÓN

Generalmente **la legislación sobre certificación digital ha ido, como en otros muchos aspectos tecnológicos, siempre por detrás de los avances del mercado, aunque hoy en día esta cuestión se ha estabilizado**. En la actualidad, esa legislación que hasta hace unos años era una de las barreras más importantes en el desarrollo de aspectos clave en torno a la certificación digital ha dejado de ser un impedimento y se ha convertido en un impulso para el mismo.

Actualmente **la legislación existente es suficientemente amplia** y se trata ahora de, cumpliendo lo establecido en la ley, explicar al ciudadano qué es lo que puede hacer de una manera sencilla y clara y elaborar sistemas de información que garanticen que cualquier usuario pueda utilizar el entorno que desee garantizando el principio de interoperabilidad y de neutralidad tecnológica. La legislación actual ha supuesto la eliminación de barreras e imponen una serie de retos muy importantes en materia de certificación digital aunque siempre respecto a las obligaciones de la administración.

El objetivo es ahora **conseguir, al menos a nivel estatal, desarrollar una normativa común** puesto que un exceso de leyes y reglamentaciones a nivel de ayuntamientos, comunidades autónomas,… podría provocar inseguridad jurídica. La legislación actual contiene todavía conceptos no demasiado claros por lo que su aplicación, en algunos aspectos, es diversa.

En este aspecto se destacan como puntos clave la Ley 59/2003, del 19 de diciembre, que equipara la firma electrónica con la firma manuscrita, y la Ley 11/2007, del 22 de junio, que obliga a la Administración Pública a dotarse de los medios y sistemas electrónicos que posibiliten a los ciudadanos a ejercer su derecho a comunicarse con las Administraciones por medios electrónicos y el Real Decreto 1671/2009, por el que se desarrolla parcialmente la citada Ley 11/2007 en el ámbito de la Administración General del Estado.

Los derechos de los ciudadanos reconocidos en la Ley 11/2007, del 22 de junio, que obliga a la Administración Pública a poner todos los servicios ofrecidos en Internet todavía no son los suficientemente conocidos y entendidos a nivel ciudadanía, aunque ya se reconoce hoy en día el papel pionero de España en el reconocimiento de los derechos del ciudadano a través de Internet.

La legislación existente actualmente pone los pilares claves de la gestión de identidades, del documento electrónico con garantías jurídicas, del archivo documental,… que ahora deberán evolucionar sincronizando aspectos tan diversos como el tecnológico, el de regulación y el de procedimientos.

8. ANEXOS

8.1. Anexo I: Legislación y normativa

8.1.1. LEGISLACIÓN AUTONÓMICA

- **Decreto 198/2010, de 2 de diciembre, por el que se regula el desarrollo de la Administración electrónica en la Xunta de Galicia y en las entidades de ella dependientes**

  Artículo 1º.-Objeto

  Este decreto tiene por objeto regular el derecho de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos, la tramitación de los procedimientos administrativos incorporados a la tramitación telemática, la creación y regulación de la sede electrónica, la creación de la edición electrónica del Diario Oficial de Galicia y del Registro Electrónico, el impulso y desarrollo de los servicios electrónicos y el establecimiento de infraestructuras y servicios de interoperabilidad.

  REFERENCIA:

  http://www.xunta.es/doc/dog.nsf/75f326159e4790474125664400367b9e/443297d14c4be22fc12577fb005dcb4e/$FILE/24100D001P006.PDF

- **Orden de 12 de febrero de 2010 por la que se regulan los procedimientos del sistema electrónico de facturación de la Xunta de Galicia**

  Artículo 1º.-Objeto

  Esta orden tiene por objeto desarrollar, al amparo del artículo 15 del Decreto 3/2010, por el que se regula la factura electrónica y la utilización de medios electrónicos, informáticos y telemáticos en materia de contratación pública de la Administración de la Comunidad Autónoma de Galicia y entes del sector público de ella dependientes, los procedimientos de tramitación de facturas en el sistema electrónico de facturación con la finalidad de ofrecer un punto de referencia único a los empresarios o profesionales que están obligados a expedir factura por las entregas de bienes y prestaciones de servicios que realicen en el desarrollo de su actividad.

  REFERENCIA:

  http://www.xunta.es/Dog/Dog2010.nsf/FichaContenido/5412?OpenDocument

8.1.2. LEGISLACIÓN ESTATAL

- **Ley 59/2003, de Firma Electrónica**

  Artículo 1. Objeto.

  1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

  2. Las disposiciones contenidas en esta ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

  REFERENCIA:

  http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf

- **Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos**

  Artículo 1. Objeto de la Ley

  1. La presente Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

  2. Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

  REFERENCIA:

  http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf

- **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**

Artículo 1. Objeto y ámbito de aplicación.

1. El presente real decreto tiene por objeto desarrollar la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos en el ámbito de la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta, en lo relativo a la transmisión de datos, sedes electrónicas y punto de acceso general, identificación y autenticación, registros electrónicos, comunicaciones y notificaciones y documentos electrónicos y copias.

2. Sus disposiciones son de aplicación:

a) A la actividad de la Administración General del Estado, así como de los organismos públicos vinculados o dependientes de la misma.

b) A los ciudadanos en sus relaciones con las entidades referidas en el párrafo anterior.

c) A las relaciones entre los órganos y organismos a los que se refiere el párrafo a).

REFERENCIA:

http://www.boe.es/boe/dias/2009/11/18/pdfs/BOE-A-2009-18358.pdf

- **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**

Artículo 1. Objeto.

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley.

2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

REFERENCIA:

http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interope-

rabilidad en el ámbito de la Administración Electrónica

Artículo 1. Objeto

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Interoperabilidad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica.

REFERENCIA:

http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf

- **Ley Orgánica 15/1999, de Protección de Datos Personales**

Artículo 1. Objeto

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

REFERENCIA:

http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

- **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal**

Artículo 1. Objeto

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad

de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

REFERENCIA:

http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

- **LEY 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información**

REFERENCIA:

http://www.boe.es/boe/dias/2007/12/29/pdfs/A53701-53719.pdf

OTRA LEGISLACIÓN Y NORMATIVA NACIONAL

- Orden ITC/1475/2006, de 11 de mayo, sobre utilización del procedimiento electrónico para la compulsa de documentos en el ámbito del Ministerio de Industria, Turismo y Comercio. (BOE 16-05-2006)

- Orden EHA/3636/2005, de 11 de noviembre, por la que se crea el registro telemático del Ministerio de Economía y Hacienda. (BOE 24-11-2005)

- Orden ITC/3928/2004, de 12 de noviembre, por la que se crea un registro telemático en el Ministerio de Industria, Turismo y Comercio. (BOE 01-12-2004)

- Orden HAC/1181/2003, de 12 de mayo, (BOE 15-05-2003) por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria

- Resolución de 24 de julio de 2003 de la Dirección General de la Agencia Estatal de Administración Tributaria por la que se establece el procedimiento a seguir para la admisión de certificados de entidades prestadoras de servicios de certificación electrónica

- Orden ECO/2579/2003, de 15 de septiembre, por la que se establecen normas sobre el uso de la firma electrónica en las relaciones por medios electrónicos, informáticos y telemáticos con el Ministerio de Economía y sus Organismos adscritos.

- 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.

8.1.3. LEGISLACIÓN COMUNITARIA

- **Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.**

- **Decisión de la comisión de 14 de julio de 2003 relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE de Parlamento Europeo y del Consejo.**

- **Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior (Directiva Bolkestein).**

- **Norma europea "ETSI 101 456: Requisitos para la política de certificación de las autoridades de certificación que emiten certificados reconocidos".**

- **Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.**

8.2. Anexo II: Referencias y bibliografía

"El manual práctico de supervivencia en la Administración Electrónic@"

Alberto López Tallón

Primera Edición – Septiembre 2010 (edición revisada)

ISBN: 978-84-614-3413-8

<http://www.microlopez.org/downloads/Manual_Supervivencia_eAdmin.pdf>

NOTA: Esta obra se publica en la modalidad de Reconocimiento-No comercial-Compartir bajo la licencia 3.0 España de Creative Commons

"La factura electrónica"

Manuales Plan Avanza

ISBN: 84-611-4740-5

<http://www.planavanza.es/Canales/Pymes/Documents/ManualFacturaElectronica%201-55.pdf>

PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA (MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO):

<https://www11.mityc.es/prestadores/busquedaPrestadores.jsp>

8.3. Anexo III: Glosario de términos

Activación

Es el procedimiento por el cual se desbloquean las condiciones de acceso a un clave y se permite su uso. En el caso de la tarjeta del DNIe el dato de activación es la clave personal de acceso (PIN) y/o los patrones de las impresiones dactilares (biometría).

Agencia de Protección de Datos --APD

Organismo oficial creado en España en 1993 como consecuencia de la aprobación de la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal). Su finalidad es proteger a los ciudadanos contra las invasiones de su intimidad realizadas mediante medios informáticos, según establece el artículo 18.4 de la Constitución Española.

Algoritmo criptográfico

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 permiten el uso de cifras seguras para la producción y comprobación de la firma electrónica.

API (Application Programming Interface - Interfaz de Programación de Aplicaciones)

Grupo de rutinas (conformando una interfaz) que provee un sistema operativo, una aplicación o una biblioteca, que definen cómo invocar desde un programa un servicio que éstos prestan. En otras palabras, una API representa un interfaz de comunicación entre componentes software.

El software que provee la funcionalidad descrita por una API se dice que es una implementación del API. El API en sí mismo es abstracto, en donde especifica una interfaz y no da detalles de implementación.

Archivo con extensión ".CSR"

Son las siglas de "Certificate Signing Request", que quiere decir "Solicitud de certificación". Un archivo de solicitud de certificación indica cuál es la clave pública a certificar y cuáles son los datos: nombre, atributos, etc.

Archivo con extensión ".p12" o "pfx"

Estos ficheros contienen un certificado digital, junto con la clave privada correspondiente y los certificados de todas las autoridades de certificación hasta la que es la raíz (o, como se suele decir, la cadena de certificación).

Autenticación

Procedimiento de comprobación de la identidad de un solicitante o titular de certificados de DNIe.

Autenticidad documental electrónica

La autenticidad es una propiedad del documento electrónico que nos informa del hecho de que el documento tenga unas determinadas características.

Autoridad de certificación (AC)

Una autoridad de certificación es un sistema informático dedicado a la emisión y gestión posterior de certificados digitales, incluyendo la renovación, expiración, suspensión, la habilitación y la revocación de certificados, a petición de la autoridad de registro. La emisión de certificados se hace de una forma automatizada y no sin la previa confirmación de la autoridad local de registro. Son funciones básicas de las autoridades de certificación: 1) verificar la identidad de los solicitantes de certificados y 2) publicar las listas de revocación de certificados.

Autoridad de sellado de fecha y hora

Una autoridad de sellado de fecha y hora (en inglés TSA, Time Stambping Authority) es un sistema informático dedicado a las funciones de emisión de sellos de fecha y hora criptográficos en las condiciones necesarias de calidad y seguridad, y en concreto, de la gestión de la fuente fiable de fecha y hora, que debe estar sincronizada con la hora oficial.

Autoridad de validación

Es el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación.

Cadena de certificados

Las cadenas de certificados permiten que los empleados públicos de dos administraciones públicas se envíen documentos firmados y verifiquen correctamente las firmas.

Caducidad

Los certificados tienen un periodo de validez determinado. Una vez éste ha pasado, si no ha sido renovado, el certificado deja de estar operativo y por tanto, deja de estar vigente.

Certificado de autenticación

Tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá a través de su certificado acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen, por tanto los terceros aceptantes y los prestadores de servicios no tendrán garantía del compromiso del titular del DNI con el contenido firmado. Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).

Este certificado puede ser utilizado también como medio de identificación para la realización de un registro que permita la expedición de certificados reconocidos por parte de entidades privadas, sin verse estas obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

Certificado digital

Un certificado digital es un documento electrónico firmado por una autoridad de certificación, que garantiza a las terceras personas que lo reciben o lo utilizan una serie de manifestaciones en él contenidas, como por ejemplo, la identidad de la persona, las autorizaciones, su capacidad para realizar un determinado acto, etc.

El certificado digital permite a las partes tener confianza en las transacciones en Internet, por tanto, garantiza la identidad de su poseedor en Internet mediante un sistema seguro de claves administrado por una tercera parte de confianza, la autoridad de certificación. El certificado permite realizar un conjunto de acciones de forma segura y con la validez legal: firmar documentos, entrar en lugares restringidos, identificarse frente la administración, etc.

Certificado reconocido

Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Certificados de identidad pública

Emitidos como Certificados Reconocidos, vinculan una serie de datos personales del ciudadano a unas determinadas claves, para garantizar la autenticidad, integridad y no repudio. Esta información está firmada electrónicamente por la Autoridad de Certificación creada al efecto.

Cifra criptográfica

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

Cifrado

Es el proceso que se aplica a unos datos para hacerlos incomprensibles y evitar que puedan ser observados por otras personas. Este proceso o transformación precisa de una clave de cifrado, que es una cadena aleatoria de bits. Sólo aplicando el proceso contrario, denominado descifrado, a los datos cifrados será posible regenerar los datos originales (y, por tanto, hacerlos otra vez comprensibles).

Esta segunda transformación precisa de una clave de descifrado determinada, y que será la misma clave de cifrado si se trabaja dentro de un sistema de claves simétricas, o de otra clave matemáticamente relacionada, complementaria, de la clave de cifrado, cuando se trabaja dentro de un sistema de claves asimétricas.

Ciudadano

Toda persona física con nacionalidad española que solicita la expedición o renovación de un Documento Nacional de Identidad ante un funcionario de la Dirección General de la Policía.

Clave criptográfica

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.

Clave pública

La clave pública es necesaria para comprobar la identidad del emisor o la autenticidad de un documento firmado. Permite validar una firma que haya sido generada con la clave privada complementaria.

La clave pública es el único elemento del certificado digital que se puede encontrar al alcance de cualquiera. Las claves públicas están disponibles en directorios publicados en Internet y en algún caso en bases de datos corporativas. Se relaciona, mediante procedimientos matemáticos, con otro elemento (clave privada) para garantizar su confidencialidad e integridad. La clave pública sirve básicamente para cifrar, aunque también se utiliza para verificar firmas digitales.

Cualquier persona puede cifrar un mensaje utilizando la clave pública, pero sólo el poseedor de la clave privada puede descifrarlo.

Clave privada

La clave privada es el elemento secreto del certificado. Está relacionado, mediante procedimientos matemáticos, con otro elemento (clave pública). La clave privada se guarda en la tarjeta inteligente de la persona certificada y, por tanto, tiene todas las garantías de seguridad, aunque se pueda encontrar en repositorio o en llave USB. Sirve, básicamente, para descifrar los mensajes recibidos, aunque también se utiliza para crear la firma digital.

Clave de sesión

Clave que establece para cifrar una comunicación entre dos entidades. La clave se establece de forma específica para cada comunicación, sesión, terminando su utilidad una vez finalizada ésta.

Clave personal de acceso (PIN)

Secuencia de caracteres que permiten el acceso a los certificados.

Cloud Computing

Informática en la Nube. Tipo de tecnología de los servicios informáticos que permiten tener acceso a todo tipo de información y servicios desde la red sin necesidad de tener discos duros.

La computación en nube es un concepto que incorpora el software como servicio, tal como la Web 2.0 y otros recientes, también conocidos como tendencias tecnológicas, donde el tema en común es la confianza en Internet para satisfacer las necesidades de cómputo de los usuarios.

CPS (prácticas de certificación)

Las Prácticas de Certificación recogen los procedimientos y requerimientos mínimos para la emisión de certificados digitales a los cuales se ajustan los prestadores de servicio de certificación. En la CPS se especifica también como se realiza el mantenimiento de una infraestructura de clave pública basada en Certificados. En definitiva, la CPS detalla y concreta el proceso completo de certificación.

Datos de creación de firma (clave privada)

Son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la Firma electrónica.

Datos de verificación de firma (clave pública)

Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma electrónica.

Directorio

Repositorio de información que sigue el estándar X.500 de ITU-T.

Dispositivo seguro de creación de firma

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

Documento electrónico

Conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información.

Documento de seguridad

Documento exigido por la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal cuyo objetivo es establecer las medidas de seguridad implantadas, a los efectos de este documento, por la DGP como Prestador de Servicios de Certificación, para la protección de los datos de carácter personal contenidos en los Ficheros de la actividad de certificación que contienen datos personales (en adelante los Ficheros).

Encargado del tratamiento

La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento de los ficheros.

Entidad de certificación

Persona física o jurídica que emite certificados, de acuerdo con la Ley de firma electrónica. En ocasiones se trata como un sinónimo de autoridad de certificación, que es un componente técnico del servicio.

Firma digital

Una firma digital es una transformación matemática de un documento, realizada mediante una operación de cifrado asimétrico con la clave privada del firmante.

Firma electrónica

La firma electrónica es un concepto legal, neutral desde una perspectiva tecnológica, que da cobertura al uso de cualquier tecnología que permita obtener las mismas funciones, con técnicas electrónicas, informáticas y telemáticas, que la firma de documentos en soporte papel.

La Ley 59/2003 de firma electrónica reconoce tres tipos de firma electrónica, en función del certificado digital que la genera: firma electrónica ordinaria, firma electrónica avanzada y firma electrónica reconocida, esta última equiparada a la firma manuscrita.

Firma electrónica avanzada

Es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

Firma electrónica reconocida

Es aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Firma envolvente

Es modalidad de firma electrónica que incluye el documento que se ha firmado, envolviéndolo. Cuando el formato de firma es CMS (Cryptographic Message Syntax) o CAdES (CMS Advanced Digital Electronic Signature) se traduce como "attached"; si el formato de firma es XMLdSIG (XML digital Signature) o XAdES (XML Advanced digital Electronic Signature) se traduce "enveloping".

Firma envuelta (enveloped)

Es una firma XMLdSIG (XML digital Signature) y XAdES (XML Advanced digital Electronic Signature) tal que el elemento signature está contenido, envuelto, dentro del elemento firmado. El caso más común es cuando el elemento a firmar es el node raíz del documento.

Firma separada (detached)

Modalidad de firma electrónica que no incluye el documento que se ha firmado. Si la firma es CMS o CAdES se almacenan por separado, en ficheros diferentes, la firma y el documento que se ha firmado. Cuando es XMLdSIG o XAdES, la firma hace referencia a un elemento externo, al XML, o bien, la posición del elemento firmado y el node firma no implica la inclusión en ninguno de los dos sentidos.

Firmas desatendidas

Las que se generan mediante un proceso automático yi sin la intervención de ningún operador. Es necesario que los datos de creación de firma estén almacenados en un servidor.

Fuente de tiempo fiable

Una fuente fiable de fecha y hora es un sistema informático que nos informa de la hora y la fecha reales, en tiempo universal coordinado, utilizado por la emisión de sellos de fecha y hora criptográficos. Típicamente se utiliza el suministrado por el ROA (Real Instituto y Observatorio de la Armada).

Funciones hash o de resumen

Una función hash es una operación matemática de resumen que se aplica a un conjunto de datos o mensaje. Esta operación permite obtener un resumen asociado a los datos generales y garantiza que no sean posibles dos mensajes diferentes con un "resumen" hash idéntico. Gracias a esta función las comunicaciones electrónicas pueden realizarse más rápidamente porque la medida de los datos es menor y pesan menos, con lo cual se agiliza la transmisión de datos. Siempre que se disponga del conjunto de datos iniciales se puede obtener el resumen, pero desde el resumen no se puede obtener los datos iniciales.

Garantía de la firma electrónica

La garantía de la firma electrónica la facilita el prestador de servicios de certificación en relación con la calidad de los algorismos, de las claves y de su funcionamiento conjunto y correcto con el resto de elementos necesarios para producir firmas electrónicas.

Habilitación

La habilitación consiste en volver a activar un certificado que ha sido suspendido. Esta habilitación siempre se ha de solicitar expresamente y en un plazo máximo de 120 días desde la fecha de la suspensión.

Hash o Huella digital

Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

HSM (módulo de seguridad hardware)

Es un dispositivo hardware con capacidades criptográficas que permiten generar i almacenar de manera segura claves criptográficas - típicamente, les datos de creación de firmas (claves privadas utilizadas en PKI). Para que sea considerado Dispositivo Seguro de Creación de Firma (conforme a lo que establece el artículo 24 de la Ley 59/2003, de 19 de diciembre, de signatura electrónica) tendrá que cumplir con los requisitos establecidos por la especificación técnica CEN CWA 14169 o equivalente (según la Decisión de la Comisión de 14 de julio de 2003 relativa a la publicación de los nombres de referencia de les normas con reconocimiento general para productos de signatura electrónica, de conformidad con lo que se dispone en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo).

Identificación

Procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados de DNIe.

Identificador de usuario

Conjunto de caracteres que se utilizan para la identificación unívoca de un usuario en un sistema.

Jerarquía de confianza

Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una AC de nivel superior garantiza la confiabilidad de una o varias de nivel inferior. En el caso de DNIe, la jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.

Listas de revocación de certificados (o listas de certificados revocados)

Lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

Módulo criptográfico hardware de seguridad

Módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

PKI - "Public Key Infrastructure"

Expresión referente a toda la infraestructura necesaria para poder poner en marcha y explotar sistemas y aplicaciones que utilizan técnicas de criptografía asimétrica. La criptografía asimétrica consiste en asignar dos claves a diferentes usuarios para que en sus comunicaciones electrónicas puedan descifrar la clave el otro usuario y así certificar su identidad.

Prestador de servicios de certificación

Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Prestador de servicios de sellos de fecha y hora

Un prestador de servicios de certificación que emite sellos de fecha y hora es una persona física o jurídica que produce y firma en nombre suyo los sellos de fecha y hora. Por tanto, legalmente es el responsable de la calidad y seguridad del sello de tiempo y responde de los daños que cualquier persona pueda sufrir en caso de confiar en los sellos.

Prueba de la firma electrónica

La prueba de la firma electrónica es el soporte donde se encuentran los datos firmados que serán admisibles como prueba documental en un juicio.

Punto de actualización del DNIe

Terminal ubicado en las Oficinas de Expedición que permite al ciudadano de forma guiada, sin la intervención de un funcionario, la realización de ciertas operaciones con el DNIe (comprobación de datos almacenados en la tarjeta, renovación de los certificados de Identidad Pública, cambio de clave personal de acceso – PIN - , etc.).

Renovación

La renovación consiste en solicitar un nuevo certificado mediante un certificado vigente pero que está a punto de caducar. De esta manera, durante los dos meses anteriores a la caducidad de un certificado se puede solicitar la renovación y esto implica que se emita un nuevo certificado válido.

Revocación

Anulación definitiva de un certificado digital a petición del suscriptor, o por propia iniciativa de la autoridad de certificación en caso de duda de la seguridad de las claves. La revocación es un estado irreversible. Se puede solicitar la revocación de un certificado después de una situación de suspensión o por voluntad de las personas autorizadas a solicitarla. De la misma manera, en el caso de un certificado suspendido, si ha pasado el periodo de suspensión máximo, si el certificado no ha sido habilitado, pasa a estar definitivamente revocado. Cuando la entidad de certificación revoca o suspende un certificado, ha de hacerlo constar en las Listas de Certificados Revocados (CRL), para hacer público este hecho. Para verificar el estado de un certificado se debe consultar la CRL publicada más recientemente de la entidad de certificación que emitió el certificado en el cual se desea confiar. Estas listas son públicas y deben estar siempre disponibles.

Sellado de tiempo

Un sello de tiempo o sello de fecha y hora, concretamente, es un documento que nos indica la fecha y hora en que se ha producido un acto, mediante una fuente de tiempo fiable de fecha y hora. El servicio de sellado de tiempo permite asociar un documento a una fecha y hora, y de esta manera obtener evidencias (técnicas y jurídicas) de que tal acto se ha producido antes de un determinado momento del tiempo.

Solicitante

Persona que solicita un certificado para sí mismo.

Suspensión

Invalidación temporal de un certificado digital como consecuencia de la petición del suscriptor, o por propia iniciativa de la autoridad de certificación, en caso de duda sobre la seguridad de las claves.

Tercero Aceptante

Persona o entidad diferente del titular que decide aceptar y confiar en un certificado.

Titular

Ciudadano para el que se expide un certificado de identidad pública.


Colexio Profesional de
Enxeñaría en Informática
de Galicia
CPEIG


Fundación para o Fomento
da Calidade Industrial e
o Desenvolvemento
Tecnolóxico de Galicia


plan
avanza2


XUNTA
DE GALICIA