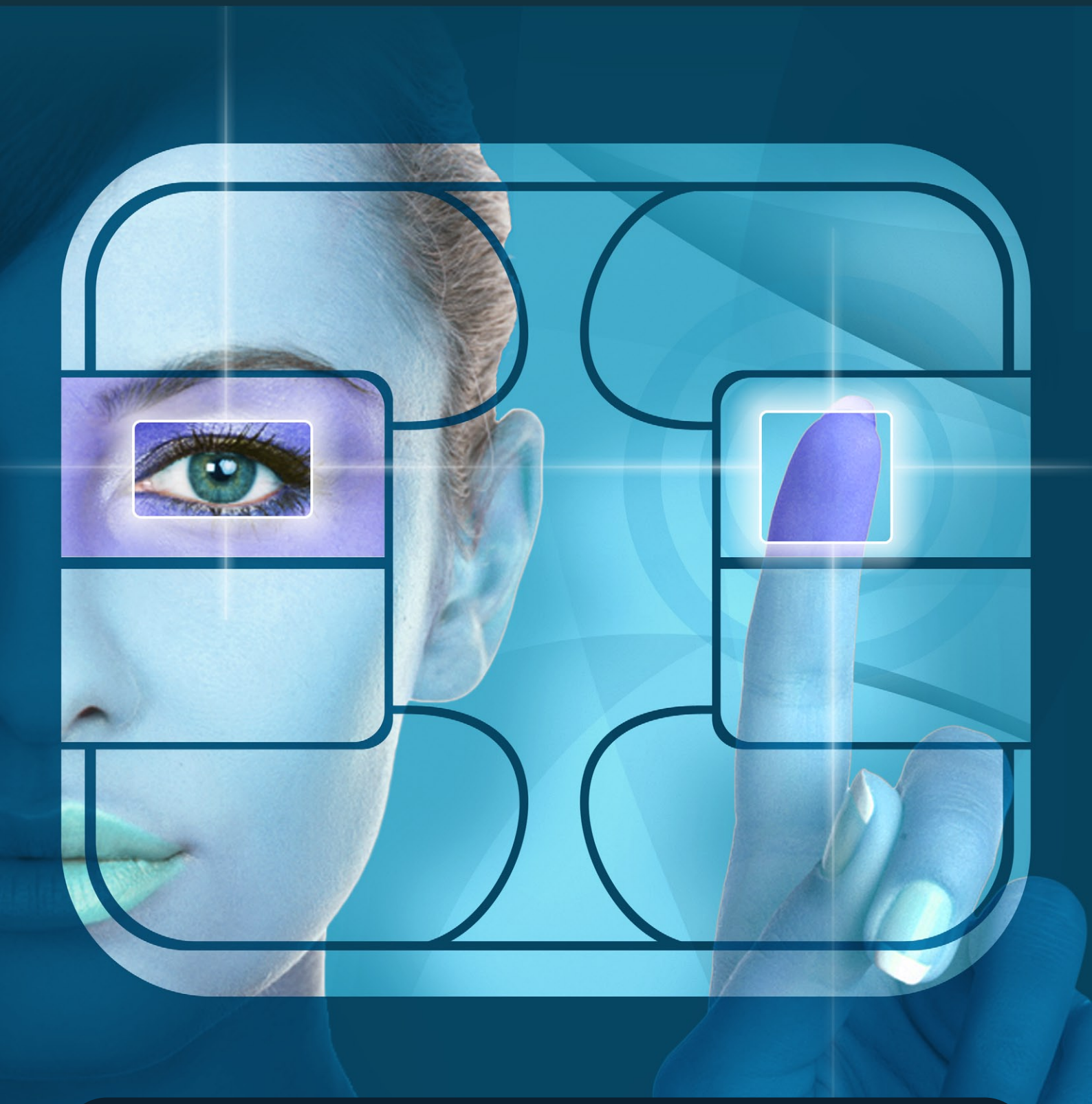


Construíndo a identidade dixital

Situación actual da sinatura electrónica e das entidades de certificación

Colexio Profesional de Enxeñaría en Informática de Galicia

coa colaboración da 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

Ano de publicación: 2011

ISBN 978-84-614-6073-1

PRÓLOGO

A Xunta de Galicia entende a Administración electrónica coma un xeito de ofrecer aos cidadáns e ás empresas uns servizos públicos máis eficientes e próximos mediante a utilización das tecnoloxías da información. Hoxe non se concibe unha Administración eficiente sen os novos mecanismos e dispositivos de xestión pública que proporcionan as TIC, sistemas transparentes de traballo e servizo e a coordinación e colaboración entre os distintos niveis administrativos.

Sabemos que as TIC axilizan as xestións administrativas evitando a cidadáns e empresas moitas cargas e desprazamentos innecesarios. Non obstante, dada a súa grande incidencia nos procesos de modernización administrativa, temos que subliñar a importancia de garantir a identidade e a confidencialidade dos trámites realizados entre os cidadáns, as empresas e as administracións. É por iso que o Goberno galego está a abordar desde esta perspectiva a mellora da súa propia xestión interna no marco das iniciativas impulsadas pola Axenda Dixital 2014.gal.

O Consello da Xunta de Galicia aprobou o día 2 de Decembro de 2010 o Decreto que establece o marco de desenvolvemento da Administración electrónica na Administración pública galega. Esta nova norma regula, entre outros aspectos, a creación da sede electrónica da Xunta, a formalización do rexistro electrónico, a xestión dixital dos procedementos administrativos e documentos electrónicos, os medios para a acreditación de cidadáns e empregados públicos neste novo contexto electrónico. O obxectivo é avanzar na mellora da calidade e da eficacia dos servizos ofrecidos, logrando unha maior eficiencia interna e nas relacións intra e interadministrativas. Trátase de conseguir unha Administración máis transparente e aberta aos cidadáns as 24 horas os 365 días do ano.

Non podemos esquecer que a Administración local é a máis próxima ao cidadán. Non é posible a consolidación da Administración electrónica se non se consigue que sexa unha realidade tamén nos concellos. É obriga das administracións públicas a cooperación, a coordinación, o aproveitamento de esforzos e de recursos. A prestación dos servizos de acreditación dixital e sinatura electrónica é un deses servizos que a Xunta pon a disposición do resto das entidades públicas galegas (concellos, deputacións provinciais, universidades galegas...) o que lles permitirá aforrar custos para avanzar na implantación da Administración electrónica.

Con iniciativas como esta, a Xunta está a impulsar a adaptación da Administración autonómica aos requirimentos da Lei 11/2007 de acceso electrónico dos cidadáns aos servizos públicos, que obriga ás administracións a favorecer relacións seguras e accesibles, garantindo de maneira efectiva o dereito dos cidadáns a relacionarse coa Administración por medios electrónicos.

Galicia sitúase como a terceira Comunidade Autónoma con maior uso da Administración electrónica para obter información das páxinas web e a quinta Comunidade en descarga e cumprimentación de formularios oficiais. Estes datos indican que temos unha boa base para afrontar os cambios e os futuros retos da Sociedade da Información. Por iso, na actualidade resulta imprescindible xerar con-

fianza nas relacións electrónicas (comunicacións, trámites, transaccións...), contando con sistemas de acreditación, como a sinatura, que permitan verificar a identidade das persoas con idéntico valor que a sinatura manuscrita.

Resulta imprescindible difundir entre os cidadáns e as empresas toda a información sobre o estado actual da sinatura electrónica e da certificación dixital, incluíndo as autoridades e entidades prestadoras de servizos de certificación. É por iso que a Secretaría Xeral de Modernización e Innovación Tecnolóxica se congratula de colaborar co Colexio Profesional de Enxeñaría en Informática de Galicia nesta iniciativa para a difusión do coñecemento existente nunha materia tan sensible para o desenvolvemento dos novos produtos e servizos da Sociedade da Información.

Santiago de Compostela, Xaneiro 2011

Mar Pereira Álvarez

Secretaria Xeral de Modernización e Innovación Tecnolóxica

Presidencia – Xunta de Galicia

PRÓLOGO

As últimas décadas do pasado século e o comezo do presente estiveron marcadas por unha verdadeira "Revolución Dixital", debida aos cambios producidos polo impacto das Tecnoloxías da Información e o Coñecemento (TIC) en todos os ámbitos da sociedade actual. Ademais, estas transformacións, caracterízanse pola velocidade á que se incorporan a todas as esferas da nosa vida, cambiando o noso xeito de comunicarnos, organizarnos, traballar e mesmo divertirnos.

Neste proceso de cambio, toma especial protagonismo a Internet, como paradigma da interconexión total. A súa difusión e uso van moito máis aló das súas orixes militares, empregándose na actualidade dos xeitos máis diversos que poidamos imaxinar: busca de información, punto de encontro, promoción persoal e profesional, medio de comunicación e mesmo lugar de lecer e compras.

O termo Sociedade da Información mostra, polo tanto, o protagonismo que as TIC están a adquirir no mundo actual; pero se imos un pouco máis aló, podemos comezar a falar da Sociedade do Coñecemento, facendo referencia non só á capacidade de acceso a volumes inxentes de información, senón tamén á facilidade de manipulación de esta e as posibilidades de interacción e colaboración con outras persoas, superando toda limitación temporal e espacial.

É un feito que as TIC (moitas veces chamadas, ao meu entender de xeito erróneo, Novas Tecnoloxías, xa que o concepto de novidade leva consigo unha connotación de temporalidade, superada pola vertixe da súa evolución) están asociadas á innovación. Calquera nova tecnoloxía ten como obxectivo a mellora e superación das características da súa predecesora; non obstante, no caso das TIC, non só se busca completar as existentes, senón mesmo potencialas e revitalizalas.

Nesta nova sociedade, o avance tecnolóxico vai moito máis aló da conexión á Internet dende un ordenador. O cambio implica unha evolución dos roles sociais, a cultura, o coñecemento e a información. Como xa se mencionaba antes, coñecemento e información constitúen os piares da sociedade do futuro.

Nesta transformación tecnolóxica global, na que a acumulación e manexo da información se produce de xeito masivo, as relacións electrónicas están a adquirir maior presenza e relevancia. A xeración de confianza neste novo medio de interacción tanto persoal coma comercial é crucial para que chegue a todos os estratos sociais e económicos da nosa sociedade. É neste aspecto onde a sinatura electrónica está a tomar máis relevancia cada día.

A sinatura electrónica xorde da necesidade das empresas e administracións de reducir os custos e, sobre todo, de aumentar a seguridade dos seus procesos internos. Deste xeito, eríxese como unha ferramenta fundamental para a mellora da seguridade da información e a xeración de confianza, posto que permite efectuar unha comprobación da identidade da orixe e da integridade das mensaxes intercambiadas na Internet. A súa condición de inmodificable achega un grao superior de seguridade.

Este libro pretende constituírse en obra de referencia para a consulta sobre o estado actual da sinatura electrónica. Ao longo do texto vaise avanzando dende os conceptos máis básicos relativos á propia firma e os certificados dixitais ata unha visión de futuro sobre os retos que debe abordar en canto a difusión, servizos e seguridade. Os diferentes capítulos van debullando elementos fundamentais como o DNI electrónico, os principais prestadores de servizos existentes en España, os servizos ofrecidos en relación a esta nova modalidade de sinatura e a fundamental relación que se establece arredor da Administración electrónica. Abórdase, ademais, un pequeno repaso sobre cuestións legais, así como a principal normativa existente que lle afecta á materia.

Non se trata, polo tanto, dunha obra conclusa, senón que a idea é que sexa actualizable no noso afán de convertela en referente sobre a situación actual en todo momento sobre o uso, implicacións e beneficios da sinatura electrónica.

Dende o CPEIG somos conscientes da relevancia que na nova Sociedade do Coñecemento toma a Enxeñaría en Informática e de que unha das súas principais funcións debe ser a divulgativa. É preciso estender o coñecemento das novas ferramentas, técnicas e normativas para facer universal o uso dos servizos xurdidos arredor das TIC. O uso de estas implica comprender a realidade social en que se vive, afrontar a convivencia e os conflitos empregando o xuízo ético baseado nos valores e prácticas democráticas e exercer a cidadanía actuando con criterio propio. Este coñecemento e actitude contribuirá á construción da paz e a democracia, e ao mantemento dunha actitude construtiva, solidaria e responsable ante o cumprimento dos dereitos e obrigas cívicas. En definitiva, o emprego das TIC constitúe o elemento tractor fundamental para a mellora da calidade de vida.

Santiago de Compostela, Xaneiro 2011

Fernando Suárez Lorenzo

Presidente do Colexio Profesional de Enxeñaría en Informática de Galicia

Contido

GRUPO DE TRABALLO

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

INTRODUCIÓN

O obxectivo principal deste traballo é difundir entre a cidadanía e as empresas boa parte do coñecemento existente en materia de sinatura electrónica e certificación dixital, incluíndo as autoridades e entidades prestadoras de servizos de certificación. Para este fin, este estudo realiza unha análise da situación actual, os avances máis significativos e os retos que se nos presentan de cara ao futuro no ámbito da identidade dixital.

Este traballo é froito da colaboración entre a Secretaría Xeral de Modernización e Innovación Tecnolóxica da Xunta de Galicia e o Colexio Profesional de Enxeñaría en Informática de Galicia (CPEIG), a través do convenio asinado polo CPEIG e a Fundación para o Fomento da Calidade Industrial e Desenvolvemento Tecnolóxico de Galicia, no marco das iniciativas impulsadas pola Axenda Dixital 2014.gal.

A metodoloxía empregada neste estudo baseouse principalmente na elaboración de entrevistas mantidas cos responsables dalgunhas das principais organizacións públicas e privadas que traballan arredor da sinatura electrónica e a certificación dixital, xunto á análise de datos e indicadores, lexislación e documentación de referencia.

O primeiro capítulo ofrece unha introdución conceptual ao ámbito da identidade dixital.

O segundo capítulo aborda a visión estratéxica dos expertos sobre os aspectos máis relevantes relacionados coa certificación dixital e a sinatura electrónica.

O terceiro capítulo recolle unha panorámica dos servizos e produtos ofrecidos actualmente polas organizacións, públicas e privadas, máis representativas no sector da certificación dixital e a sinatura electrónica en España.

O cuarto capítulo ofrece unha análise experta da lexislación existente na materia.

O quinto capítulo fai unha breve análise dos principais indicadores estatísticos relacionados coa certificación dixital e a sinatura electrónica.

O sétimo capítulo reúne as conclusións.

1.

¿QUE É A IDENTIDADE DIXITAL?

A tecnoloxía cobra cada vez un papel máis relevante nas nosas vidas e fai que pouco a pouco nos incorporemos a un universo tecnolóxico onde a nosa identidade dixital transcorre paralela á nosa identidade física.

Dende sempre, a capacidade para identificar os individuos ou as organizacións non estivo exenta de polémica, non obstante chegamos á utilización de sistemas consensuados e validados de identificación, como os documentos de identidade ou os pasaportes, que ninguén pon en dúbida, aínda cando existan certos perigos residuais na súa utilización.

No mundo tecnolóxico estamos aínda nunha fase temperá de identificación, de feito podemos crear contas de correo electrónico gratuítas, perfís en redes sociais, abrir *blogs* ou *twittear* sen ningún tipo de validación sobre a nosa entidade física. Por outra banda, a maior parte de organizacións (como banca ou *utilities*) ofrécenlles servizo en liña aos seus clientes, utilizando sistemas heteroxéneos de identificación e validación.

En España, dende o ano 2006, estase a emitir un documento nacional de identidade que incorpora un certificado electrónico, o que engade un nivel de seguridade á relación dos cidadáns tanto coas administracións públicas coma con outras entidades privadas. Neste caso, o Ministerio del Interior actúa como terceiro de confianza ou autoridade de certificación.

En España, e como experiencias previas á aparición do DNI electrónico, existe un número importante de autoridades de certificación que emiten certificados electrónicos de diversos tipos e funcionan como terceiros de confianza sobre a base do seu cumprimento das garantías de acreditación que fixan, tanto a Lei 30/1992, do 26 de novembro, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común (modificada pola Lei 4/1999, de 13 de xaneiro), como na Lei 11/2007 de acceso electrónico dos cidadáns aos Servizos Públicos nas súas relacións coa Administración. Entre os tipos de certificados máis usados están:

- Certificados individuais, referidos tanto a persoas coma a entidades:
    - Certificado persoal, que acredita a identidade do titular.
    - Certificado de pertenza á entidade, que ademais da identidade do titular acredita a súa vinculación coa entidade para a que traballa.
    - Certificado de representante, que ademais da pertenza á empresa acredita tamén os poderes de representación que o titular ten sobre esta.
    - Certificado de persoa xurídica, que identifica unha empresa ou sociedade como tal á hora de realizar trámites ante as administracións ou institucións.
    - Certificado de atributo, o cal permite identificar unha calidade, estado ou

situación.

- Certificados técnicos, utilizados para identificación de servidores ou sistemas de información:
    - Certificado de servidor seguro, utilizado nos servidores web que queren protexer ante terceiros o intercambio de información cos usuarios.
    - Certificado de sinatura de código, para garantir a autoría e a non modificación do código de aplicacións informáticas.
- Certificados para Administración pública, definidos na Lei 11/2007, do 22 de xuño, de Acceso Electrónico dos Cidadáns aos Servizos Públicos:
    - Sede electrónica, simplificando, para identificar os sitios web das administracións públicas.
    - Selo electrónico (ou de órgano), para a actualización administrativa automatizada.
    - De empregado ao servizo da Administración pública, para a identificación e sinatura de persoas físicas ao servizo da Administración pública.

O obxectivo de todo iso é proporcionarlles aos cidadáns e organizacións unha identidade dixital segura e equipar a súa seguridade e garantías de e-cidadán ás de cidadán.

A Lei 59/2003 de Firma Electrónica incorpora ao dereito español a normativa legal europea en materia de sinatura electrónica, concretamente a Directiva 1999/93/CE, pola que se establece un marco comunitario para a sinatura electrónica. A devandita lei regula aspectos referentes a:

- prestadores de servizos de certificación, establecendo que non está suxeita a autorización previa e se realizará en réxime de libre competencia.
- DNI electrónico como medio de identificación, que acredita electronicamente a identidade e permite a sinatura electrónica.
- certificados electrónicos e sinatura electrónica recoñecida.
- dispositivos de creación de sinatura e de verificación de sinatura.
- réxime de supervisión e control, e infraccións e sancións.

1.1. Sinatura electrónica recoñecida

A Lei 59/2003 no seu artigo 3 outórgalle á sinatura electrónica recoñecida respecto dos datos consignados en forma electrónica o mesmo valor que á sinatura manuscrita en relación cos datos consignados en papel, podendo dar soporte a documentos públicos e privados.

Artigo 3. Sinatura electrónica, e documentos asinados electronicamente.

1. A sinatura electrónica é o conxunto de datos en forma electrónica, consignados xunto a outros ou asociados con eles, que poden ser utilizados como medio de identificación do asinante.

2. A sinatura electrónica avanzada é a sinatura electrónica que permite identificar o asinante e detectar calquera cambio ulterior dos datos asinados, que está vinculada ao asinante de xeito único e aos datos a que se refire e que foi creada por medios que o asinante pode manter baixo o seu exclusivo control.

*3. Considérase **sinatura electrónica recoñecida** a sinatura electrónica avanzada baseada nun certificado recoñecido e xerada mediante un dispositivo seguro de creación de sinatura.*

4. A sinatura electrónica recoñecida terá respecto dos datos consignados en forma electrónica o mesmo valor que a sinatura manuscrita en relación cos consignados en papel.

5. Considérase documento electrónico a información de calquera natureza en forma electrónica, arquivada nun soporte electrónico segundo un formato determinado e susceptible de identificación e tratamento diferenciado.

Sen prexuízo do disposto no parágrafo anterior, para que un documento electrónico teña a natureza de documento público ou de documento administrativo deberá cumprirse, respectivamente, co disposto nas letras a ou b do apartado seguinte e, no seu caso, na normativa específica aplicable.

6. O documento electrónico será soporte de:

a. *Documentos públicos, por estar asinados electronicamente por funcionarios que teñan legalmente atribuída a facultade de dar fe pública, xudicial, notarial ou administrativa, sempre que actúen no ámbito das súas competencias cos requisitos esixidos pola lei en cada caso.*

b. *Documentos expedidos e asinados electronicamente por funcionarios ou empregados públicos no exercicio das súas funcións públicas, conforme á súa lexislación específica.*

c. *Documentos privados.*

Define, ademais, que unha sinatura electrónica recoñecida é considerada unha sinatura electrónica avanzada baseada en certificado recoñecido, e xerada mediante dispositivo

seguro de creación de sinatura.

Así mesmo, nos artigos 6 e 11 da mesma lei, considérase certificado electrónico recoñecido a aquel que é expedido por un prestador de servizos de certificación que cumpra os requisitos de comprobar a identidade e circunstancias persoais dos solicitantes de certificados, verificar que toda a información contida no certificado é exacta, asegurarse de que o asinante está en posesión dos datos de creación de sinatura correspondentes aos de verificación que constan no certificado e garantir a complementariedade dos datos de creación e verificación de sinatura, sempre que ambos os dous sexan xerados polo prestador de servizos de certificación.

Para verificar se un certificado é recoñecido, pódese visitar a web do Ministerio de Industria, Turismo y Comercio, onde se publican os prestadores de servizos de certificación baseados en certificados recoñecidos

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

Artigo 6. Concepto de certificado electrónico e de asinante.

1. Un certificado electrónico é un documento asinado electronicamente por un prestador de servizos de certificación que vincula uns datos de verificación de sinatura a un asinante e confirma a súa identidade.

2. O asinante é a persoa que posúe un dispositivo de creación de sinatura e que actúa en nome propio ou en nome dunha persoa física ou xurídica á que representa.

Artigo 11. Concepto e contido dos certificados recoñecidos.

1. Son certificados recoñecidos os certificados electrónicos expedidos por un prestador de servizos de certificación que cumpra os requisitos establecidos nesta Lei en canto á comprobación da identidade e demais circunstancias dos solicitantes e á fiabilidade e as garantías dos servizos de certificación que presten.

2. Os certificados recoñecidos incluirán, polo menos, os seguintes datos:

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

b. *O código identificativo único do certificado.*

c. *A identificación do prestador de servizos de certificación que expide o certificado e o seu domicilio.*

d. *A sinatura electrónica avanzada do prestador de servizos de certificación que expide o certificado.*

e. *A identificación do asinante, no suposto de persoas físicas, polo seu nome e apelidos e o seu número de*

documento nacional de identidade ou a través dun pseudónimo que conste como tal de xeito inequívoco e, no suposto de persoas xurídicas, pola súa denominación ou razón social e o seu código de identificación fiscal.

f. *Os datos de verificación de sinatura que correspondan aos datos de creación de sinatura que se encontren baixo o control do asinante.*

g. *O comezo e o fin do período de validez do certificado.*

h. *Os límites de uso do certificado, se se establecen.*

i. *Os límites do valor das transaccións para as que pode utilizarse o certificado, se se establecen.*

O outro requisito que debe cumprir unha sinatura electrónica recoñecida é a súa xeración mediante un dispositivo seguro de sinatura, e a el dedícase o artigo 24 na súa totalidade, indicando que os datos utilizados para a xeración da sinatura deben xerarse só unha vez, asegurando o seu segredo e protexéndoos de xeito fiable polo asinante, garantindo, ademais, que o dispositivo utilizado non altere os datos ou o documento que deba asinarse nin impida que este se lle mostre ao asinante antes do proceso de sinatura. Esta garantía do dispositivo debe ser emitida por entidades de certificación recoñecidas tal e como se detalla no artigo 27.

Artigo 24. Dispositivos de creación de sinatura electrónica.

1. Os datos de creación de sinatura son os datos únicos, como códigos ou claves criptográficas privadas, que o asinante utiliza para crear a sinatura electrónica.

2. Un dispositivo de creación de sinatura é un programa ou sistema informático que serve para aplicar os datos de creación de sinatura.

3. Un dispositivo seguro de creación de sinatura é un dispositivo de creación de sinatura que ofrece, polo menos, as seguintes garantías:

a. *Que os datos utilizados para a xeración de sinatura poden producirse só unha vez e asegura razoablemente o seu segredo.*

b. *Que existe unha seguridade razoable de que os datos utilizados para a xeración de sinatura non poden ser derivados dos de verificación de sinatura ou da propia sinatura e de que a sinatura está protexida contra a falsificación coa tecnoloxía existente en cada momento.*

c. *Que os datos de creación de sinatura poden ser protexidos de forma fiable polo asinante contra a súa utilización por terceiros.*

d. *Que o dispositivo utilizado non altera os datos ou o documento que deba asinarse nin impide que este se lle mostre ao asinante antes do proceso de sinatura.*

Artigo 27. Certificación de dispositivos seguros de creación de sinatura electrónica.

1. A certificación de dispositivos seguros de creación de sinatura electrónica é o procedemento polo que se comproba que un dispositivo cumpre os requisitos establecidos nesta Lei para a súa consideración como dispositivo seguro de creación de sinatura.

2. A certificación poderá ser solicitada polos fabricantes ou importadores de dispositivos de creación de sinatura e levarase a cabo polas entidades de certificación recoñecidas por unha entidade de acreditación designada de acordo co disposto na Lei 21/1992, do 16 de xullo, de Industria e nas súas disposicións de desenvolvemento.

3. Nos procedementos de certificación utilizaranse as normas técnicas cuxos números de referencia fosen publicados no Diario Oficial da Unión Europea e, excepcionalmente, as aprobadas polo Ministerio de Ciencia y Tecnología que se publicarán na dirección de Internet deste Ministerio.

4. Os certificados de conformidade dos dispositivos seguros de creación de sinatura serán modificados ou, no seu caso, revogados cando se deixen de cumprir as condicións establecidas para a súa obtención.

Os certificados electrónicos teñen un período de validez de acordo coas características e tecnoloxía empregada para a súa xeración, e, no seu caso, os certificados recoñecidos non poderán ter un período de validez superior a catro anos.

1.2. DNI electrónico

O Documento Nacional de Identidade foi evolucionando durante máis de 50 anos, incorporando continuas innovacións para garantir tanto a seguridade do documento como o ámbito de aplicación. Nos últimos anos, e, co obxecto de darlles cobertura ás necesidades do mundo dixital, xurdiu o novo Documento Nacional de Identidade electrónico (DNIe), que incorpora un *chip* capaz de gardar de xeito seguro información e de procesala internamente.

Con este novo dispositivo somos capaces de acreditar electronicamente e, sen lugar a dúbida, a identidade da persoa, así como de asinar dixitalmente documentos electrónicos, outorgándolles unha validez xurídica equivalente á sinatura manuscrita.

Como viamos no capítulo anterior, o DNIe proporciona unha sinatura electrónica recoñecida, posto que é considerada unha sinatura electrónica avanzada baseada nun certificado recoñecido, emitido polo Ministerio del Interior e xerada mediante dispositivo seguro de creación de sinatura.

Este novo DNIe proporciona importantes vantaxes sobre o DNI convencional, que podemos resumir en:

- Ampliar a nosa capacidade de actuar telematicamente coas administracións públicas, coas empresas e con outros cidadáns.
- Realizar transaccións bancarias asinadas a través da Internet.
- Accesos a instalacións ou a sistemas informáticos.
- Realizar accións a través da Internet (compras, conversacións, etcétera) con garantías de que o interlocutor é quen di ser.

Por todo o exposto, as vantaxes do DNIe son moi claras, tanto dende o punto de vista de seguridade coma de comodidade, e mesmo de ergonomía, posto que fisicamente é un documento máis robusto e ten unha duración prevista de dez anos.

2.

A OPINIÓN DO SECTOR

O impulso que a identidade dixital viviu en España non sería tan significativo, como o é actualmente, sen o apoio e a implicación das organizacións, públicas e privadas, que desenvolven e traballan nas áreas de negocio, cada vez máis diversas e relevantes, en torno a esta tecnoloxía.

Nas entrevistas que a continuación presentamos, mantidas cos responsables dalgunhas destas organizacións, podemos coñecer que opinan da situación actual, dos avances máis representativos e, sobre todo, das necesidades e retos de cara ao futuro.

Da súa experiencia e do seu coñecemento poderemos extraer importantes conclusións de cara ao futuro da identidade dixital, un ámbito no que actualmente España ocupa unha posición privilexiada e no cal débese seguir traballando de xeito intenso para poder mantelo.

Neste apartado inclúese, ademais, para establecer o contexto das organizacións participantes en este, unha pequena reseña corporativa da historia e obxectivos de cada unha de elas. Como se comentou xa anteriormente, aínda que se tiveron en conta para o estudo moitas entidades e empresas, tanto públicas coma privadas, para a selección das entidades analizadas de xeito máis detallado seguíronse diversos criterios de relevancia dos servizos ofrecidos, volume de certificados xestionados ou produtos máis innovadores.

2.1. Agència Catalana de Certificació

A Agència Catalana de Certificació (CATCert) nace no ano 2002 como organismo autónomo ao abeiro do Consorcio Administració Oberta de Catalunya. O seu obxectivo é proporcionarlles ás administracións catalás os instrumentos necesarios para que as transaccións electrónicas a través da Internet teñan todas as garantías xurídicas e velar para que o proceso do despregamento da sinatura electrónica na Administración sexa o máis amigable posible.

As novas tecnoloxías fixeron posible a interacción e a transacción de servizos e procedementos en liña. O impulso das administracións catalás para aplicarlles estas tecnoloxías ás relacións interadministrativas e entre Administración e cidadán permítelles ofrecer un servizo mellor e máis áxil, ao tempo que supón unha iniciativa innovadora no sector público.

Unha vez regulado o marco xurídico xeral e establecida a validez dos documentos e das comunicacións telemáticas o uso de certificados recoñecidos permitirá garantir a identidade das partes implicadas, así como a confidencialidade, a integridade e o non rexeitamento dos documentos e das xestións realizadas.

O conxunto de servizos ofrecido pola Agència Catalana de Certificació conforma o sistema público catalán de certificación.

A misión da Agència Catalana de Certificació-CATCert é prestar servizos de sinatura electrónica para as administracións catalás. Como tal, garantirá a confidencialidade, a integridade, a identidade e o non rexeitamento nas comunicacións e transaccións electrónicas que se realicen no ámbito das administracións públicas catalás.

A Agència Catalana de Certificació estableceu como principais obxectivos os seguintes:

- Ofrecerlles ás administracións catalás os instrumentos necesarios para asegurar que os trámites a través da Internet teñan todas as garantías xurídicas.
- Proporcionarlle ao persoal das administracións catalás diferentes tipos de certificados dixitais avalados pola Administración.
- Facilitar o desenvolvemento de aplicacións e servizos que requiran o uso da sinatura electrónica.
- Velar para que o proceso de despregamento da sinatura electrónica na Administración sexa o máis sinxelo posible.

2.1.1. Entrevista con Xavier Tarrés Chamorro

Xavier Tarrés Chamorro

Director Xeral

Agència Catalana de Certificació (CATCert)

Xavier Tarrés Chamorro: "A certificación dixital é un avance imparable que axuda á modernización da Administración Pública e leva consigo unha optimización de recursos fundamental para loitar contra a crise"

O director de la Agència Catalana de Certificació (CATCert) destaca o importante papel que tivo o organismo como impulsor de certificados dixitais e servizos de valor engadido nun momento "en que había que empezar a predicar no deserto"

Para Tarrés Chamorro está xustificada a creación dun organismo propio de certificación en Cataluña e afirma que o seu alcance non só debe medirse en clave económica, senón tamén en termos políticos e organizativos

O gran reto de futuro do certificado dixital é, segundo Tarrés Chamorro, lograr que o seu uso sexa tan doado e transparente que se converta en invisible

"Este avance imparable que supoñen as novas tecnoloxías e a certificación dixital axudan á modernización da Administración pública, o que leva consigo unha optimización de recursos, un dos piares fundamentais para loitar contra esta crise," afirma o director da Agència Catalana de Certificació (CATCert), Xavier Tarrés Chamorro. Para el, a e-Administración é o futuro, forxado a base dos impresionantes avances tecnolóxicos que se pon a disposición da cidadanía e tamén ao día a día da Administración pública. Tal como expón, a tecnoloxía chega a todas as partes, e tamén aos cidadáns, que cada vez esixen máis para que a propia Administración ofreza servizos telemáticos.

Da man destes avances no mundo tecnolóxico xorde no ano 2002 a Agència Catalana de Certificació (CATCert) como organismo autónomo ao abeiro do Consorcio Administració Oberta de Catalunya e coa participación nun 60 por cento da Generalitat de Catalunya en nun 40 por cento do mundo local a través de LocalRed. Dende a súa posta en marcha ten un obxectivo claro: proporcionarlles ás administracións catalás os instrumentos necesarios para que as transaccións electrónicas a través da Internet dispoñan de todas as garantías xurídicas, ao tempo que vela polo proceso de despregamento da sinatura electrónica na Administración. O conxunto dos servizos ofrecidos por CATCert conforman o coñecido como Sistema Público Catalán de Certificación.

Fronte aos que apostan por un modelo de unidade en materia de autoridade de emisión de certificacións dixitais, o máximo responsable de CATCert defende a proposta catalá que tivo, segundo apunta, "un papel de impulso importante, tanto a nivel de certificados como de servizos de valor engadido", especialmente nun momento -no que naceu- no que aínda non había mercado, nin regulación, nin necesidades. "Había que empezar a predicar no deserto", recorda.

"O momento en que se constitúe CATCert creo que foi unha decisión moi acertada", asegura Xavier Tarrés Chamorro, quen explica que, aínda que economicamente se gastou máis diñeiro fronte á alternativa de *outsourcing* de servizos, este investimento fixo que a situación actual en Cataluña sexa "moito máis avanzada que noutras comunidades por impulso do coñecemento, por capacidade independente de dirixir as políticas de Administración electrónica ou por nivel actual de implantación, entre outras". "A aceptación de CATCert como autoridade permite estar fortes no despregamento da e-Administración en Cataluña", apunta Tarrés Chamorro.

Neste punto, o responsable de CATCert explica que a evolución en materia de certificación dixital supuxo que a súa entidade pasase de moverse nun mercado de oferta (Só CATCert e FNMT lles ofrecían servizos ás administracións) a un mercado de demanda, xa que agora son as propias administracións locais e autonómica as que cada vez máis solicitan unha carteira de servizo máis ampla e con acordos de nivel de prestación de servizos moi esixentes.

A Agència Catalana de Certificació ten un triplo rol. Tal como explica o seu director, é unha autoridade prestadora de servizos de certificación como terceiro de confianza, segundo os ditados da Lei de Firma Electrónica, que ademais ofrece servizos de valor engadido que axudan a utilizar, estender e fomentar a identidade dixital e a sinatura electrónica. Ademais, o organismo ofrece servizos de acompañamento e asesoramento co obxectivo de que a fenda dixital se reduza o antes posible. Con este encargo, CATCert estrutúrase de xeito interno en tres áreas clave: área de certificación e calidade; área técnica; e área de asesoría e innovación.

Rendibilidade futura

Consultado sobre o retorno do investimento realizado na posta en marcha dunha autoridade de certificación propia en Cataluña, Xavier Tarrés Chamorro teno claro: "O retorno do investimento é moi difícil de calcular", pero recalca que a rendibilidade desta iniciativa non debe medirse unicamente en termos económicos. Neste punto, fai referencia á situación actual que se vive na Comunidade, cunha economía a escala; cunha estratexia de Administración electrónica forte e que mantén a identidade propia; cunha rede coordinada con protocolos e ritmo de despregamento propios; e na que a cooperación entre administracións se ve reforzada cunha posición forte para aplicar os servizos de identidade e documento electrónicos, en especial cando se teñen calendarios propios e coordinados entre todas

as administracións da Comunidade. Para el isto fai ver que o retorno do investimento realizado no CATCert "é político, no sentido de que é consecuencia dunha decisión estratéxica que é gañadora seguro".

Segundo os datos que manexa Tarrés Chamorro, ata o momento CATCert emitiu xa preto de 160.000 certificados de cidadán _otros 60.000 de empregado público_ e máis de 1.500 de servidor ou dispositivo, cos servizos necesarios que estes levan asociados. O presuposto anual do organismo ascende aos 5 millóns de euros e conta cun equipo composto por 31 persoas.

Usos do certificado dixital

Segundo apunta o director do CATCert, existe unha diferenza importante entre Europa e España no uso do certificado dixital xa que, mentres que en Europa o motor de promoción desta tecnoloxía foi a banca, en España foi a Agencia Tributaria. Ademais, destaca o labor "moi importante" de impulso do certificado electrónico en Cataluña realizado dende as cámaras de comercio e dende o ámbito profesional. Aínda así, para Tarrés Chamorro o papel clave xógao, sen lugar a dúbidas, a Administración pública, tanto por volume de traballadores públicos e de necesidades de automatización certificada coma polo seu papel de tractor de empresas e cidadanía. "Se a administración ofrece servizos importantes para o usuario a través da Web seguro que o cidadán vai utilizalos", apunta, ao tempo que recorda que tamén os mozos ocupan un papel relevante neste impulso, "pola súa visión e capacidade tecnolóxica e porque xa empezan a ocupar postos relevantes e con poder de decisión nas empresas".

Para Xavier Tarrés Chamorro "o mercado do certificado dixital é aínda incipiente, a pesar de que o noso país conta cunha vintena de prestadores. A alfabetización dixital -escasa- da nosa poboación, as dificultades de comprensión destas tecnoloxías e o estado aínda incipiente da "vida dixital" dos negocios e as transaccións no ámbito da Internet fan necesaria unha optimización das aplicacións de cara a un uso "amigable e compatible con todos os sistemas". Tamén que a oferta de certificados á poboación final poida estenderse de forma masiva. "É un peixe que se morde a cola".

Concretamente no caso de CATCert, Tarrés Chamorro recorda que o organismo lles presta servizos de certificación ás administracións públicas e tamén ofrece certificados dixitais para os cidadáns, o equivalente a o que emite a Fábrica Nacional de Moneda y Timbre (FNMT). Pola contra, CATCert non orientou os seus servizos ás empresas "para non interferir nun mercado libre que ofrece xa servizos e que está os suficientemente maduro".

Lexislación dixital

No referente á situación lexislativa actual en materia de certificación dixital, Xavier Tarrés Chamorro

móstrase contrariado. Segundo explica, as leis actuais supuxeron a eliminación de barreiras e impoñen unha serie de retos en materia de certificación dixital, "pero sempre respecto á obriga da Administración". Así, ao seu xuízo os dereitos dos cidadáns recoñecidos na Lei 11/2007, do 22 de xuño, que lle obriga á Administración pública a poñer todos os servizos ofrecidos na Internet, aínda non son os suficientemente coñecidos e entendidos a nivel cidadanía. "Serán as novas xeracións as que realmente os demanden", considera, nun futuro no que si se recoñecerá o papel pioneiro de España no recoñecemento dos dereitos do cidadán a través da Internet.

A pesar do importante avance que supón esta lei, nela non se abordan os procesos automatizados que unha operación desta magnitude debe levar asociados, segundo explica Tarrés Chamorro. A pesar disto, gaba o feito de que a normativa "poña a alfombra á xestión de identidades, ao documento electrónico con garantías xurídicas, ao arquivo documental, en definitiva, á vía dixital". "A vía dixital da Administración pública ten que evolucionar sincronizando camiños tan diversos como o tecnolóxico, o de regulación e o de procedementos," engade.

Para Tarrés Chamorro a lexislación, que antes era unha das grandes barreiras para a Administración electrónica e para o uso de certificados dixitais como infraestrutura básica desta e-Administración, xa non é hoxe en día un impedimento para os avances dixitais senón máis ben un impulso. Na actualidade, as barreiras á Administración electrónica veñen impostas pola usabilidade das propias tecnoloxías e polo cambio cultural e de hábitos que esta nova Administración require.

Ao concretar a aplicación da Lei 11/2007, do 22 de xuño, en Cataluña, Xavier Tarrés Chamorro considera que, nestes momentos, Generalitat e concellos grandes e medios se encontran na fase de despregamento da normativa, avanzando claramente cara a unha consolidación de esta. Pola contra, son os pequenos concellos os que se encontran nunha posición máis retraída. Neste punto, recorda que existe unha estratexia de infraestrutura rural definida pola propia Generalitat para levar a banda larga ao medio rural, favorecendo así a implantación dos servizos dixitais nos municipios con maiores dificultades. Para Tarrés Chamorro é unha estratexia necesaria porque a implantación electrónica necesita ir ao mesmo tempo cá implantación de infraestruturas.

Neste punto, Tarrés Chamorro achegou a innovadora experiencia posta en marcha en Cataluña, onde se emitiu unha normativa que obriga aos concellos a enviar electronicamente as súas contas e actas de goberno. Un total de 947 administracións locais comezaron xa a operar con este sistema, que funciona a través dunha plataforma intermedia e que supón o uso de certificacións dixitais, coa total validez xurídica que leva consigo e o aforro de tempo, intermediarios, erros, arquivo físico e gastos de transporte.

Retos de futuro

O futuro pasa pola tecnoloxía, pola aplicación das tecnoloxías aos procesos de xestión dos servizos públicos. Pero aínda que o certificado dixital se presente como unha das grandes solucións tecnolóxicas das próximas xeracións, sen a cal non é posible despregar a vía dixital, para o director da Agència Catalana de Certificació é necesario ter en conta problemas como a preservación da sinatura electrónica no tempo, posto que é de obrigado cumprimento manter a súa continuidade e validez. Para iso, explica, CATCert desenvolveu unha plataforma de xestión documental cun selo de perdurabilidade que aborda estas necesidades. Este pode ser un dos moitos retos aos que se enfronta o mundo dixital. "A medida que avanzamos encontrámonos con novos problemas nesta vida dixital que iniciamos", reflexiona Xavier Tarrés Chamorro.

Nesta liña, Tarrés Chamorro aborda igualmente o obxectivo principal do organismo que dirixe. A súa finalidade é seguir desenvolvendo o seu traballo actual, sen intención inicialmente de converterse en provedor de servizos para outras comunidades e outros organismos fóra de Cataluña, "porque podería interpretarse como unha competencia do ámbito empresarial". Saber xestionar esta premisa con éxito é, para Tarrés Chamorro, a clave para evitar conflitos de intereses coas entidades privadas, garantindo a pervivencia futura de ambos os dous tipos de organismos. Outro tipo de colaboración interadministrativa para a mellora ou aceleración na implantación de sistemas de certificación dixital sempre é posible.

Ademais, é consciente de que a implantación definitiva do DNIe supoñerá, a medio ou longo prazo, o fin dos certificados de cidadán que CATCert emite actualmente. "En España temos a gran sorte de contar coa axuda do DNIe de cara ao cidadán, aínda que necesita mellorar a súa usabilidade", subliña. Este é, sen dúbida, o gran reto ao que se enfronta a certificación dixital de cara ao futuro: conseguir que o uso dos certificados dixitais sexa tan doado e transparente que se faga invisible para o cidadán.

Sobre a situación de España en materia de certificación dixital en contraste con Europa, Xavier Tarrés Chamorro recorda que o marco lexislativo é común, aínda que afirma que os servizos de interoperabilidade aínda deben evolucionar. Neste sentido traballouse a nivel europeo no proxecto STORK, para conseguir o recoñecemento paneuropeo das identidades electrónicas; e a nivel español na creación dunha liña TSL´s, ou listas de confianza interoperables entre estados membros. "Pero é un camiño a longo prazo", detalla. Ademais, recorda que dende Europa se identifican ás infraestruturas de identidade dixital como ferramentas clave para saír da crise, unha grande oportunidade pero á vez un gran reto para os países.

Por outra parte, segundo Tarrés Chamorro, para España é moi importante, dende o punto de vista económico, ser interoperables con países de Latinoamérica, "posto que son vías de negocio para os

provedores de servizo españois".

"A oportunidade de cara ao futuro é que a vía dixital está a crecer, e é necesario ofrecer solucións de acordo ás necesidades que están a crecer", conclúe Xavier Tarrés Chamorro, confiado nas posibilidades de España, como país, de facer fronte aos grandes retos aos que se enfronta xa na era dixital.

2.2. Albalia Interactiva

Albalia Interactiva é unha empresa de Consultaría e Servizos, de capital español, creada en 1997, con experiencia en ámbitos de alta tecnoloxía bancarios e de telecomunicacións.

Entre as súas especializacións están a seguridade, sinatura electrónica, factura electrónica, Administración electrónica, banca electrónica, medios de pagamento e mobilidade.

O enfoque seguido é de "Tecnoloxía Legal". É dicir, Albalia leva a cabo un intenso seguimento de todos os avances lexislativos que teñen implicacións tecnolóxicas no ámbito tanto das entidades financeiras coma noutros tipos de empresas nos que este enfoque sexa significativo. Deste xeito descóbrense interesantes posibilidades que poden ser aproveitadas polas entidades máis avanzadas ou máis preocupar polo servizo ao cliente e, noutras ocasións, identifícanse normas que implican obrigas para as entidades, o que se engloba nas necesidades de "Compliance" ou cumprimento normativo.

Albalia Interactiva desenvolve proxectos de Hacking *Etico*, *mystery shopping*, Factura electrónica, UBL, XBRL, Siantura electrónica, *Mobipay*, DNI dixital, PDF intelixente, Voto electrónico, LOPD-LSSI, UNE 71502, ISO 17799, UNE 166001 e 166002, e-notario créditos persoais, e-notario hipotecario, tarxetas intelixentes, PKI, *Single Sign On*, Evidencias Electrónicas e Análise Forense.

2.2.1. Entrevista con Julián Inza Aldaz

Julián Inza Aldaz

Presidente

Albalia Interactiva

Julián Inza: "O noso valor engadido fundamental é a seguridade xurídica que achegamos en todos os procesos con documentos dixitais"

O presidente de Albalia Interactiva destaca como peculiaridade da compañía a sinerxía con empresas do grupo, en función das accións que realiza: de consultoría, de formación e de desenvolvemento de produtos e servizos.

Para Inza a complexidade das implementacións prácticas do uso do DNI electrónico

están a atrasar o cambio esperado respecto ao descoñecemento ou indiferenza da cidadanía ante a certificación dixital.

A seguridade xurídica que ofrece Albalia Interactiva en todos os procesos nos que poida aplicarse a sinatura electrónica e certificación dixital é, segundo o presidente da entidade, Julián Inza, o valor engadido fundamental da marca. O grupo de consultoría e servizos relacionados coa certificación dixital e as novas tecnoloxías nace en 1997, como Libraría Interactiva. En 2003 créase Albalia Interactiva, enfocándose na consultoría técnica e xurídica e no desenvolvemento de solucións de seguridade, e a Libraría Interactiva transfórmase en Atenea Interactiva, a empresa do grupo especializada en formación. Albalia especialízase na seguridade, sinatura, factura, administración, comercio e banca electrónicas, así como en medios de pagamento e mobilidade. En 2009 nace EADTrust, a terceira empresa do Grupo, como PSC, Prestador de Servizos de Certificación. Especialmente dende 2003 o seu perfecto coñecemento da lei e da súa aplicación foi a clave da empresa, que ofrece aos seus clientes e usuarios esa seguridade xurídica en todas as súas accións. Ademais, outro valor que ofrece a compañía é o seu traballo como consultora e auditora en dixitalización certificada para empresas que desexan homologar as súas solucións ante a Axencia Tributaria. O proceso crea documentos dixitais a partir dos de papel e co seu mesmo valor. Ou, noutros contextos, é posible crear documentos que nacen de sinatura electrónica preservando o máximo valor probatorio, mesmo en instancias xurisdicionais centradas na presentación de probas en formato papel. "Podemos garantir que un documento electrónico ben xestionado iguala e supera en valor probatorio a un papel", explica Julián Inza.

Unha das peculiaridades do Grupo Interactiva é a súa organización estruturada en función das accións que realiza. Deste xeito, Albalia céntrase na consultoría, auditoría e prestación de servizos; Atenea Interactiva oriéntase á formación; e EADTrust é un PSC que usa e comercializa en forma de servizos os produtos desenvolvidos por Albalia. Segundo explica o presidente da compañía, o coñecemento e formación que ofrece Atenea céntrase especialmente nos campos da factura, sinatura e administración electrónicas, ademais de abordar calquera novidade legal relacionada directa ou indirectamente coa certificación dixital. O extenso e intenso labor de investigación que desenvolve esta organización permite despois aproveitar os seus avances en materia de auditoría e consultoría en Albalia. Pola súa banda, EADTrust traballa no campo do *timestamping* para completar a sinatura electrónica; na publicación fidedigna do perfil do contratante; na custodia de documentos electrónicos; na notificación fidedigna e no voto electrónico. Así, Julián Inza apunta que o Grupo ten dúas maneiras de enfocarse ao cliente: como consultora, que achega algúns produtos tecnolóxicos de confianza dixital, a través da firma Albalia, e como prestador de servizos de eConfianza na nube TIC a través de EADTrust.

O enfoque de Albalia Interactiva é de tecnoloxía legal, é dicir, dende a empresa realízase un intenso seguimento de todos os avances lexislativos que teñen implicacións tecnolóxicas no ámbito das entidades financeiras, das administracións públicas e doutro tipo de empresas nos que este enfoque sexa

significativo. Deste xeito encóntranse posibilidades interesantes que poden ser aproveitadas polas entidades máis avanzadas ou máis preocupadas polo servizo ao cliente, ao tempo que se identifican normas que implican obrigas para as entidades, o que se engloba nas necesidades de cumprimento normativo.

Usos do certificado dixital

Respecto ao uso da certificación dixital, o presidente de Albalia Interactiva teno claro, é a Administración Pública "a que está a tirar do carro" e onde máis se impulsou esta nova tecnoloxía. "Os cidadáns aínda non son conscientes da versatilidade da sinatura electrónica", asegura Julián Inza, quen considera que a Administración Pública está sendo o tractor que impulsa o desenvolvemento desta tecnoloxía e doutras conexas, como a custodia dixital representada pola sede electrónica e o código localizador CSV (Código Seguro de Verificación). De feito, para Inza a lenta adopción destas novas tecnoloxías entre a cidadanía explícanse tamén polo xeito tan complexo co que os implementadores de solucións como o rexistro electrónico ou os sistemas de interlocución telemática tratan o DNI electrónico, que provoca o rexeitamento ou indiferenza da poboación ante esta nova tecnoloxía. "Hai que facelo máis sinxelo para o usuario, cos medios actuais pódense evitar fallos exasperantes ou tarefas repetitivas sen valor" insiste Inza.

Nesta liña, Julián Inza apunta a outros campos onde o uso do certificado dixital será interesante e terá grande importancia no futuro, como son a banca, a sanidade, a universidade e as empresas denominadas "de utilities", é dicir, que ofrecen servizos de telecomunicacións, luz, auga ou gas, entre outros. Son as entidades coas que os cidadáns interactúan frecuentemente e están obrigadas a dispoñer de sistemas de "interlocución telemática" ou a garantir o dereito dos cidadáns a relacionarse con elas por medios electrónicos.

Consultado sobre a transición do mundo do papel ao mundo electrónico, o presidente de Albalia Interactiva explica que ata o momento o mecanismo básico da xestión da sinatura está sustentado en "parábolas" dixitais do mundo físico, onde o paradigma é o formato PDF, " e practicamente o pouco que se fixo no sector privado é a sinatura de ficheiros PDF". Así, recorda que estes documentos en PDF teñen moitas carencias, que os do mundo do papel non teñen, e é que dependen do concepto de documento orixinal, que non existe no mundo dixital senón como convencionalismo. E é que, segundo explica Inza, cando tes un papel orixinal ese documento ten unha serie de calidades que o transcenden: a obliterabilidade; a endosabilidade e a completitude. Nos documentos electrónicos esas calidades desvincúlanse do concepto de orixinal e xestiónanse separadamente con sistemas de custodia dixital e unha definición intelixente dos metadatos axeitados, máis próxima á xestión informática transaccional, que á documental.

Neste contexto hai que sinalar o significado destes termos. A obliterabilidade implica a posibilidade de que un documento represente un dereito e deba quedar rexistrado se se fixo uso ou non do dereito. Por exemplo, un billete de autobús cancélase ao montar no autobús e non se pode reutilizar no futuro. A endosabilidade implica a posibilidade de transferir a outro o dereito que reflicte un documento, algo relativamente doado de xestionar nos documentos nominativos e máis complexo nos documentos ao portador. O exemplo típico é o da letra de cambio ou os títulos valores (accións). A completitude é a capacidade de engadir anotacións á marxe, nos espazos libres ou engadindo follas, ou mesmo reflectindo elementos doutros documentos. Un exemplo é o dun contrato que reflicta a existencia dun anexo posterior ou un poder no que se anote posteriormente que se revogou e se asocie a unha inscrición rexistral.

Para Inza, cando só queremos dar certeza de que un documento se asinou entre as partes un PDF é un documento válido. Por iso estamos a ver que o paso do mundo do papel ao electrónico e viceversa, por exemplo no ámbito da compulsa, se está a empezar a realizar través do PDFs asinados. Pero admite que no ámbito privado aínda falta un mecanismo que permita aos particulares exercer o dereito á proba cando se trata da súa intervención en documentos electrónicos, que si poden xestionar os organismos e institucións que poñen en marcha os sistemas de relación telemática. Neste sentido, Inza destaca a interesante proposta posta en marcha polo Goberno Vasco, denominada Metaposta. Segundo a súa opinión, esta iniciativa pode evolucionar nun futuro cara a un sistema de correos electrónicos con mecanismos de custodia ou pode converterse nun dispositivo para centralizar as evidencias dos asinantes, "un modelo moi valioso". A dificultade, para Julián Inza, é que os cidadáns "aínda non interiorizaron o que supón unha sinatura electrónica no ámbito público e/ou privado".

Neste punto, Julián Inza recorda que o modelo electrónico de xestión de documentos require dous instrumentos: a sinatura electrónica e a custodia dixital. Segundo explica, a custodia dixital é esixente e complexa, xa que require a certeza a protección da información a longo prazo, e a súa dispoñibilidade ante instancias xurisdicionais, o que esixe a implantación de maiores mecanismos de seguridade; e implica a responsabilidade de organismo relacionado coa autenticidade do documento, de aí o concepto de sede electrónica. Os documentos precisan un control rigoroso de metadatos que reflicten a traza de anotacións ou vinculacións a identidades ou a outros documentos para garantir a obliterabilidade, a endosabilidade e a completitude. "A custodia dixital é máis complexa de xestionar que a sinatura electrónica que, aínda que tamén ten a súa complexidade, é unha materia na que todos temos máis experiencia", apostila.

No referente á introdución do certificado dixital no día a día dos cidadáns, o presidente de Albalia Interactiva considera que son "as xeracións novas as que realmente fomentarán o uso do certificado dixital de xeito habitual". A pesar desta optimista perspectiva de futuro, Inza tamén é consciente de que aínda "queda un tempo para madurar" e recoñece que hoxe en día só as persoas que teñen a obri-

ga ou necesidade de utilizar o documento dixital no seu día a día o fan.

Documento notarial electrónico

No referente ao documento notarial electrónico, o presidente de Albalia Interactiva explica que esta tecnoloxía está considerada tanto no actual regulamento notarial, cuxa modificación foi moi recente, en 2007, como na Lei de Acompañamento dos presupostos do ano 2002, Lei 24/2001. Así, explica que este documento está pensado para determinadas comunicacións que se realizan entre notarios e rexistros, "que é onde teñen a súa maior virtualidade". Nesta liña tamén se enmarca o concepto de protocolo electrónico, que ofrece os parámetros básicos de como se debe facer unha custodia dun documento dixital, "porque os conceptos de costura e de índice do protocolo son os mesmos que, aplicándoo ao mundo electrónico permiten a boa "levanza" da custodia dixital". Ademais, neste proceso, tal como recorda Julián Inza, os notarios, xuíces e secretarios xudiciais son figuras clave á hora de entender que é un documento electrónico, xa que son os profesionais do ámbito xurídico que máis claramente entenden o significado deste documento e os seus elementos básicos.

Para efectos prácticos actualmente aínda non se pode solicitar nunha notaría unha copia autorizada asinada electronicamente, salvo para o seu traslado a outro notario, a un rexistrador ou unha Administración pública, aínda que si unha copia simple, se o notario aprecia interese lexítimo, e esta posibilidade existe dende finais do ano 2001. É unha cuestión que, para Julián Inza, necesita aínda un tempo para a súa implantación, aínda que destaca o feito de que a día de hoxe "todos os notarios de España dispoñen da sinatura electrónica recoñecida".

Lexislación europea

O presidente de Albalia Interactiva é tallante en materia de lexislación e afirma rotundo que existe un déficit "moi grande" na Unión Europea procedente da mala aplicación do artigo 11 da Directiva 1999/93/CE do Parlamento Europeo e do Consello, pola que se establece un marco comunitario para a sinatura electrónica. Neste artigo esíxeselles aos países membros a comunicación á Comisión Europea do estado de supervisión dos prestadores de certificación dixital do seu ámbito. Malia esta obriga, Julián Inza lamenta que non se especificase de xeito claro a estrutura da información a subministrar, o que provocou que cada país o defina de xeito unilateral e envíe posteriormente a documentación á Comisión Europea. De feito, apunta que dúas cuestións clave na información a subministrar serían o certificado *root* da autoridade de certificación e o lugar onde consultar a validez dos certificados, o servizo OCSP (Online Certificate Status Protocol). Ademais, critica que, once anos despois de emitir esta directiva, se publicasen os protocolos TSL (Trust-service Status List), que deberían ter servido para facilitar o cumprimento da normativa e a elaboración dun listado común de prestadores de ser-

vizo, pero que, moi ao contrario, aínda manteñen carencias básicas, xa que, por exemplo, non inclúen información sobre os servizos de validación de cada un.

A falta de concreción da normativa europea provocou que actualmente non exista un listado común de todos os prestadores de servizos de certificación dixital de Europa, senón un simple listado de países e, dentro de cada un e nos seus respectivos idiomas, as indicacións de como encontrar cada un dos prestadores nas súas propias páxinas web. Para Inza sería necesario dispoñer dun listado normalizado para que as ferramentas, por exemplo os navegadores, teñan o camiño máis doado para buscar a información de prestadores de confianza e da validez de cada un dos seus certificados emitidos e redunde nunha mellor experiencia do usuario.

Nesta liña, o máximo representante de Albalia Interactiva apunta a unha alternativa a esta iniciativa da Unión Europea, e que consistiría nunha plataforma para acceder á lista de certificados revogados dun xeito sinxelo. Nesta cuestión "España é pioneira e está a dar un exemplo a seguir", ao que axuda o feito de que sexa o país con máis prestadores de servizos de certificación da Unión Europea e, despois de Estados Unidos, o que máis prestadores de servizos de certificación ten rexistrados nos navegadores.

Marco lexislativo español

"O ámbito de lexislación español está moito máis desenvolvido que o da maior parte doutros países do noso ámbito, é un dos mellores de Europa" "nestes momentos", expresa o presidente de Albalia Interactiva, ao tempo que concreta que este marco lexislativo está moi por diante do dos países anglosaxóns, e non tanto dos países de orixe latina, onde a necesidade da sinatura electrónica está máis clara e asumida. Aínda así, matiza que, a pesar de que hai un "bo nivel" en canto á cantidade de normativa referente a certificación dixital, se debería mellorar no referente á calidade. "Faría falta desenvolver máis os conceptos do documento electrónico, incidindo na sistemática do documento", apunta Julián Inza. Ademais, lamenta a descompensación lexislativa que existe para o sector público, con maior normativa, e para o sector privado, con menor detalle nas leis que impoñen o uso da sinatura electrónica.

Comunidades autónomas e certificación

Consultado sobre a decisión de determinadas comunidades autónomas de converterse en entidades de certificación ou prestadoras de servizos de certificación dixital, o presidente de Albalia Interactiva destaca con rotundidade a actitude que Andalucía tomou ao respecto. A pesar de non contar cunha autoridade de certificación dixital, ao seu xuízo, Andalucía entendeu ben a problemática da xestión documental electrónica, máis alá da relevancia que pode ter entre os seus organismos un prestador

de certificación propia ou non.

Por outra parte, para Julián Inza o peso que a identidade propia ten no ámbito das competencias é o que levou a comunidades como o País Vasco, a Comunidade Valencia ou Cataluña a desenvolver autoridades autónomas de certificación dixital. Neste aspecto Inza considera que en España existen iniciativas e experiencias "moi interesantes", así como profesionais altamente cualificados á fronte destas entidades autónomas. Non obstante, considera que o máis importante non é a capacidade para prestar servizos de certificación, senón a capacidade de xestionar documentos electrónicos cos servizos de certificación que xa existen, " e aí o labor máis notable foi a que desenvolveu a Administración Pública andaluza".

Retos de futuro

O presidente de Albalia Interactiva ve como "case imprescindible" o feito de que no futuro todas as Administracións Públicas dispoñan de mecanismos de xestión de documentos electrónicos e de axuda no despregamento da administración electrónica. No referente á convivencia das entidades públicas e privadas de certificación dixital, Julián Inza considera que o modelo de negocio da Fábrica de Moneda y Timbre (FNMT) debería cambiar e permitir o acceso sen custo á información de certificados revogados, o que implicaría tamén un cambio no seu mecanismo de financiamento. Por exemplo, cre que un cambio estratéxico sería incluír a CERES transitoriamente como parte da infraestrutura do Ministerio de Política Territorial e Administración Pública, o que lle proporcionaría un valor engadido moi importante a un ministerio que, segundo destaca Inza, "está a facer un labor moi interesante na súa responsabilidade de dinamizador da modernización administrativa e na apertura do mercado da certificación".

"A longo prazo tería sentido que desaparecesen as iniciativas públicas de expedición de certificados dixitais", apunta tamén Julián Inza, quen considera que as necesidades de xestión de identidades dixitais de carácter público se cubrirán co DNIe, que permitirá xestionar a maior parte das necesidades de identificación a nivel persoal. Neste punto, Inza explica que en España existen na actualidade ao redor de 26 prestadores de servizos de certificación privados e públicos, polo que "sería interesante formularse se é necesario financiar con presupostos públicos iniciativas que teñen suficiente resposta por parte do sector privado, que pola súa banda se encontra en condicións de competencia desvirtuada polas iniciativas públicas".

Neste punto, o presidente de Albalia Interactiva considera que o principal reto do futuro dixital é rematar co problema da interoperabilidade das sinaturas electrónicas en Europa, o que se alcanzaría mediante a adopción xeneralizada de formatos baseados en XML; o uso de sinaturas XADES-XL; a inclusión de áncoras de confianza, dos certificados *root* dos PSC e URL dos servizos de consultas de

revogación dos PSC nas TSL´s; e a codificación correcta do campo de consulta de certificados revogados por parte dos prestadores de servizos de certificación. E nesta mesma liña, sería tamén necesario abordar o problema da interoperabilidade dos documentos electrónicos, un reto ao seu xuízo "moi difícil" cuxa solución pasaría por crear un repositorio sincronizado de formularios XML onde todos os formatos sexan subidos polo seu creador e modificado polos usuarios que os utilicen, se detectan carencias.

Unido a esta perspectiva de futuro dixital, o responsable de Albalia Interactiva recoñece que actualmente a implantación real da factura electrónica é outro dos grandes retos aos que se enfronta o campo da certificación dixital e un avance tecnolóxico que supoñería importantes melloras de eficiencia para as empresas.

Albalia ante o futuro

Dende a súa creación, Albalia Interactiva formúlase como reto ir un paso por diante en materia de certificación dixital. Así, no plan estratéxico de futuro a compañía está a traballar a idea de crear un selo de calidade para o ámbito da dixitalización de sinaturas manuscritas, co que distinguir solucións que merecen ou non confianza, de tal xeito que se audite o sistema e avalen as solucións de xestión documental que asocian sinaturas dixitalizadas que cumpran certos principios, como a imposibilidade de reutilizar as sinaturas capturadas por parte das entidades que as captan, con comprimidos dixitalizadores ou por outros procedementos.

Ademais, entre os labores de Albalia Interactiva, Julián Inza formula a necesidade de estudar de que forma se recollen as evidencias para que a sinatura dixital teña o valor que lle outorga a lei, porque "calquera sinatura dixital non é válida". "O problema é que os usuarios non saben distinguir cando hai por detrás sistemas que ofrecen confianza ou non", lamenta.

"A Administración Pública está facendo esforzos para inculcar no cidadán esa forma de exercer os seus dereitos a través da tecnoloxía, e o sector privado poderá subirse á onda e beneficiarse diso", conclúe Inza.

2.3. Camerfirma

AC Camerfirma, S.A. foi creada no ano 1999, como un proxecto cameral co obxectivo de dotar de seguridade as comunicacións e operacións telemáticas realizadas no ámbito empresarial. Actualmente a compañía está participada polo Consello Superior de Cámaras de Comercio, por máis de 85 Cámaras de Comercio españolas e polo grupo Banesto. Ademais, forma parte de CHAMBERSIGN, entidade supranacional de ámbito europeo, que outorga recoñecemento aos seus certificados máis aló do territorio nacional.

AC Camerfirma establécese como prestador de servizos de certificación ao abeiro da Lei 59/2003, do 19 de decembro, de sinatura electrónica, é dicir como terceiro de confianza nas transaccións electrónicas, distribuíndo certificados de identidade que lles permiten ás empresas identificarse na Rede e asinar electronicamente documentos con total seguridade técnica e xurídica.

AC Camerfirma é un prestador recoñecido para a emisión de certificados ás administracións públicas sobre a base do desenvolvemento da Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos.

AC Camerfirma, dende o comezo da súa traxectoria como Sociedade Anónima no ano 2000, mantén unha estreita relación cos mercados de Sudamérica e dispón no seu labor con numerosos proxectos de consultaría e de implantación de PKI coas Cámaras de Comercio sudamericanas (Cámara de Comercio de Uruguai, Cámara de Comercio de Bogotá, Cámara de Comercio de Chile,…). A partir de 2009, Camerfirma empezou ademais a realización de proxectos de implantación de PKI en países de Europa como Portugal, Grecia,…

2.3.1. Entrevista con Rafael Román Álvarez

Rafael Román Álvarez

Responsable de Administracións Públicas

Camerfirma

Rafael Román Álvarez: "O punto forte de Camerfirma é a nosa ampla rede cameral coa que dar un bo servizo e asesoramento a empresas e administracións públicas"

O responsable de Administracións Públicas de Camerfirma destaca o feito de que a

entidade dispoña de 88 oficinas de rexistro con preto de 600 persoas con capacidade para xerar certificacións dixitais

Para Román Álvarez, un dos feitos que diferencia a súa entidade de calquera outra emisora é a validez internacional dos seus certificados dixitais

"O noso valor engadido é a ampla rede cameral que temos para darlles servizo a todas as empresas e administracións públicas. O noso punto forte é darlles un bo servizo e asesoramento, que cando compren saiban o que mercan," subliña determinante Rafael Román Álvarez, o responsable de Administracións Públicas de Camerfirma. Ese é o obxectivo e o principal motivo da creación, no ano 1999, de AC Camerfirma, un proxecto cameral que nace para dotar de seguridade as comunicacións e operacións telemáticas realizadas no ámbito empresarial. Na actualidade, a compañía está participada polo Consello Superior de Cámaras de Comercio e forma parte, ademais, de CHAMBERSING, unha entidade supranacional de ámbito europeo que lles outorga recoñecemento aos seus certificados dixitais máis aló do territorio nacional.

O valor diferencial de Camerfirma é, sen dúbida, a ampla rede de oficinas de rexistro baseadas nas cámaras de comercio das que dispoñen, un total de 88 actualmente, e as preto de 600 autoridades de rexistro coas que dispoñen en toda España, é dicir, aquelas persoas con capacidade para xerar certificados dixitais. Esta rede de recursos técese co único e principal obxectivo de darlles o mellor servizo e asesoramento aos seus clientes. Para iso Camerfirma traballa cun soporte en tres niveis: un nivel un, baseado nas preguntas básicas dos usuarios; un segundo, para a integración de sinaturas dixitais con produtos; e o terceiro, de sistemas, orientado ao desenvolvemento de produtos. Ademais, outro valor que diferenza a Camerfirma de calquera entidade similar é o seu carácter e validez internacional, porque a validez dos seus certificados dixitais se outorga a través das cámaras de comercio, organizacións que existen en todos os países do mundo.

Oportunidade de negocio

Camerfirma establécese como prestador de servizos de certificación ao abeiro da Lei 59/2003, do 19 de decembro, de sinatura electrónica, é dicir, como terceiro de confianza nas transaccións electrónicas, distribuíndo certificados de identidade que lles permiten ás empresas identificarse na Rede e asinar electronicamente documentos con total seguridade técnica e xurídica. Ademais, é prestador recoñecido para a emisión de certificados ás administracións públicas sobre a base do desenvolvemento da Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos.

Segundo explica Rafael Román Álvarez, agora Camerfirma está a tratar de estenderse a outros países, ao igual que o está a facer a Fábrica Nacional de Moneda y Timbre (FNMT), abrindo novos mercados, como en México onde se utiliza a certificación dixital para os trámites coa oficina de rexistro da pro-

piedade. “Estamos abrindo novos mercados, e nalgúns sitios xa o fixemos”, apunta.

Aínda así, a curto prazo e de xeito máis próximo a principal oportunidade de negocio que ten Camerfirma é traballar coa Administración pública, para a implantación de todos os novos sistemas. “Ata agora estanse a poñer os certificados xustos para poder poñelos en marcha, supoño que a partir do ano que vén se rematará de consolidar toda a Administración pública”.

No referente ás empresas a aposta é clara: o certificado dixital para o mundo empresarial, fomentándoo a través das cámaras de comercio. Ademais, tamén hai cabida neste proxecto de futuro para as novidades, como o *bussines wear*, co que permitirlles ás empresas avanzar en solucións propias con sinatura dixital. “Para nós tamén é unha prioridade ofrecer produtos de sinatura e factura electrónica, e estamos a traballar en iso”, conclúe.

Usos da certificación dixital

Sobre os ámbitos actuais de uso da certificación dixital, o responsable de Administracións Públicas de Camerfirma considera que ata agora se limitaba ao mundo empresarial, en trámites con Facenda ou a Seguridade Social, pero hoxe comeza a estenderse á Administración pública “e cando realmente estea implantado será a que tire por ese uso do certificado dixital”. “E esperemos que empece a tirar tamén do cidadán e do uso do DNIe” apunta. Ademais, Román Álvarez engade que cando a Administración pública remate de implantar todos os seus sistemas, as súas sedes electrónicas ou a factura electrónica, entre outros, será o momento en que se lles obrigue aos seus provedores a usar certificados dixitais e aos cidadáns a usar o DNIe, unha situación que, ao seu xuízo, non se producirá antes dun par de anos.

No referente ao uso concreto da sinatura dixital, para Román Álvarez é unha técnica pouco desenvolvida actualmente no mundo empresarial, aínda que espera que despunte coa facturación electrónica, cando a Administración pública a teña implantada e empece a esixila. “Hoxe por hoxe, no mundo empresarial, o certificado dixital coñécese e úsase só para tramitacións coa Administración pública”, sentenza. Neste sentido, explica que dende Camerfirma se desenvolveron produtos para fomentalo, como son os portais de facturación electrónica para PEMES e MicroPEMES ou os *bussinesswhere*, produtos con solucións de sinatura asociadas.

Neste punto, matízanse as diferenzas entre o certificado dixital e a sinatura electrónica. Mentres que o certificado dixital é un documento dixital mediante o cal un terceiro confiable - unha autoridade de certificación - garante a vinculación entre a identidade dun suxeito ou entidade e a súa clave pública; a sinatura dixital é aquela sinatura recoñecida e almacenada nun soporte electrónico e que ten o mesmo valor legal que a manuscrita.

Para o responsable de Administracións Públicas de Camerfirma, un dos principais motivos do pouco uso da sinatura electrónica e do certificado dixital débese ao descoñecemento que hai das súas posibilidades e garantías, tanto a nivel empresarial coma na cidadanía. "O cidadán como cidadán ten un gran descoñecemento da sinatura dixital e das tramitacións que pode facer", lamenta Román Álvarez, quen, aínda así, recoñece o esforzo que están a facer algunhas comunidades autónomas para informar a cidadanía nestes aspectos.

Neste sentido, considera que o primeiro paso debería ser axudar a empresa privada, a Administración pública e a cidadanía a distinguir sobre os distintos tipos de certificados dixitais: os emitidos pola FNMT, con uso limitado aos trámites coas administracións públicas; os certificados empresariais, emitidos por entidades privadas, que son certificados de atributos para o mundo empresarial e serven para asinar documentos como persoa pertencente a unha entidade, vinculando o traballador a esa empresa cun cargo determinado en esta; e o DNIe, para asinar documentación como cidadán. "Hai que ensinar para que é cada tipo de certificado dixital", apostila.

Certificado dixital e lexislación

A xuízo do responsable de Administracións Públicas de Camerfirma, en materia lexislativa sobre certificación dixital "temos a lei, pero aínda non hai conceptos demasiado claros, polo que a súa aplicación é diversa". Por iso, explica que as empresas optan por desenvolver os seus produtos segundo o seu criterio. Ademais, recoñece que a crise actual está a provocar unha ralentización nesta materia, sendo as empresas e as administracións públicas as que "teñen máis complicado poñerse ao día coa lei".

Por outra banda, abórdase tamén a situación actual tendente cara á homologación europea e mundial en materia de certificación dixital. Tal como explica Román Álvarez, os certificados camerales outorgados por Camerfirma teñen valor internacional, pero aínda a día de hoxe hai países que están fóra deste acordo. "A nosa validez dáse a través das cámaras de comercio, e en todos os países hai unha cámara de comercio. Esa é a que lle dá legalidade á nosa sinatura", detalla Román Álvarez, quen considera que é aquí onde se encontra un dos puntos fortes da empresa. "A nosa validez internacional é unha das grandes diferenciacións respecto a outras entidades de certificación dixital", sentenza de xeito contundente.

Comunidades autónomas como entidades de certificación

Para o membro de Camerfirma, o feito de que varias comunidades autónomas españolas se convertan en entidades de certificación dixital non é algo negativo, sempre e cando teñan unha orientación global e emitan documentos que sirvan para realizar tramitacións en calquera outra Comunidade.

Acerca da implantación da Lei 11/2007, de sinatura electrónica, Rafael Román Álvarez entende que é un proceso moi lento, xa que depende dunha serie de actuacións que estas deben realizar e que se encontran paralizadas debido á negativa conxuntura económica actual. "A sinatura electrónica é a guinda do pastel", apunta, ao tempo que explica que, só unha vez que as administracións públicas teñan implantados todos os seus procesos electrónicos na Internet, se poderá pechar o proceso coa implantación xeneralizada do certificado dixital, co que poder realizar a sinatura electrónica en todas estas tramitacións.

O futuro dixital

Consultado sobre a convivencia nun futuro das entidades públicas e privadas de certificación dixital, o responsable de Administracións Públicas de Camerfirma opina que a longo prazo unicamente se utilizarán os certificados de empregado público, que permitirán a supervivencia das entidades de certificación privadas e as comunidades autónomas; e os certificados de atributo ou empresariais, para darlles capacidade de sinatura ás empresas e organizacións; e o DNIe. "Aínda queda por vir algo novo, non sei moi ben qué, pero o DNIe ten que ir mellorándose para mellorar a impresión do usuario", matiza. Neste sentido, recorda que para o cidadán o DNIe ten como principal reto estender o seu coñecemento e uso, ademais de necesitar superar as complicacións técnicas que aínda implica o seu uso na actualidade.

2.4. Corpo Nacional de Policía (DNI electrónico)

O **Documento Nacional de Identidade electrónico** é o documento que acredita física e dixitalmente a identidade persoal do seu titular e permite a sinatura electrónica de documentos.

A súa aparencia é similar ao DNI actual, ao que se incorpora un *chip* electrónico, que contén a información básica que permita acreditar electronicamente a identidade do seu titular e a sinatura de documentos electrónicos con plena validez legal.

A principal vantaxe do DNI electrónico fronte ao convencional é que, ademais de identificar o usuario ante terceiros, permite a sinatura electrónica. O novo DNI achega seguridade, rapidez, comodidade e a inmediata realización de trámites administrativos e comerciais a través de medios telemáticos.

O *chip* que incorpora o DNI electrónico contén os mesmos datos que aparecen imprimidos na tarxeta (filiación, fotografía e sinatura dixitalizada e resumo criptográfico da impresión dactilar) xunto cos certificados de autenticación e sinatura electrónica, ademais dun certificado de compoñente propio do DNIe. O novo DNI non contén ningún dato histórico do titular como tampouco incorpora dato ningún de carácter sanitarios, fiscal, penal, laboral, etcétera.

2.4.1. Entrevista con Juan Crespo Sánchez

Juan Crespo Sánchez

Inspector Xefe

Área de Informática

Corpo Nacional de Policía

Juan Crespo: "A Administración pública española apostou polo desenvolvemento das TIC, e isto facilitou que sexamos referentes en aspectos como a identidade dixital"

O inspector xefe do Corpo Nacional de Policía destinado na área de Informática destaca a importancia do DNIe, que comezou a emitirse no ano 2006, convertendo España no cuarto país da Unión Europea que dispoñía deste novidoso dispositivo

O reto actual do DNIe é lograr que todas as aplicacións que o usan sexan certifica-

das, para transmitirlles así aos cidadáns unha sensación e realidade de seguridade a todos os niveis

No ano 2006 materialízase, como proxecto piloto, unha iniciativa coa que a Administración pública española pretende avanzar na Sociedade da Información, dotando os cidadáns dun documento de identidade electrónico: o DNI electrónico. Os primeiros pasos remóntanse ao ano 2000, cando o Goberno pon en marcha o proxecto INFO XXI para o desenvolvemento da Sociedade da Información, no que se analizan os aspectos relacionados coa seguridade dos novos servizos telemáticos. É entón cando se determina a necesidade de crear un documento de identidade electrónico co que dotar os cidadáns dun mecanismo que lles permita realizar transaccións electrónicas e interactuar de xeito seguro, así como realizar procesos de sinatura e identificación electrónica. O elemento común a todos os cidadáns era o DNI, polo que se optou por desenvolvelo nunha nova versión coa que lograr un documento válido tanto para a identificación física coma para a electrónica.

Para Juan Crespo, inspector xefe do Corpo Nacional de Policía para a área de Informática, esta aposta da Administración pública española polo desenvolvemento das TIC "facilitou que sexamos referentes en aspectos como a identidade dixital". Neste éxito non só se inclúe o DNIe, senón tamén todo o traballo realizado por diversas entidades de certificación e o desenvolvemento dos servizos relacionados necesarios por parte da Administración pública e as entidades privadas. Así, hoxe en día pódense realizar a nivel local, autonómico e estatal diferentes transaccións electrónicas cuxa garantía está avalada polo uso do DNI electrónico e doutros certificados similares. Estes avances facilítanlles aos cidadáns múltiples posibilidades nas tramitacións, con aforro de tempo e custos.

España comezou a traballar no proxecto do DNIe no ano 2001 e a experiencia piloto de expedición de documentos electrónicos concrétase no ano 2006, implantándose de xeito definitivo dous anos máis tarde. Tamén no ano 2006 empeza a expedirse, de xeito único e exclusivo, o novo pasaporte electrónico. Este documento incorpora como novidade un *chip* de radiofrecuencia que garante que os datos imprimidos non foron alterados e que coinciden cos do *chip*. Non obstante, o pasaporte electrónico funciona unicamente como elemento identificativo e carece de capacidade de sinatura.

"Fomos dos primeiros países en incorporarlle esta tecnoloxía á sociedade", subliña Juan Crespo en referencia ao DNIe. Esta aposta de España pola certificación dixital púxose de manifesto cando comezou a emitirse o DNIe, momento no que só existían experiencias similares en Finlandia, Bélxica e Estonia. Actualmente hai preto de 10 países inmersos neste proxecto, sendo Alemaña o último en incorporar documentos de identidade electrónicos, concretamente en novembro do pasado ano.

DNIe como elemento dinamizador

"O DNI electrónico non ten vocación de ser exclusivista, senón que nace con vocación de elemento

dinamizador e facilitador da Sociedade da Información e dos servizos de certificación dixital", detalla o responsable da área de Seguridade para os Sistemas Informáticos do Área de Informática do Corpo Nacional de Policía. Así, explica que a Lei 59/2003, do 19 de decembro, de Sinatura Electrónica, permite a expedición doutros certificados de sinatura electrónica baseados nun rexistro feito cun certificado xa expedido. O DNIe permite a xeración de novos prestadores de servizos de certificación sen necesidade de que despreguen oficinas de rexistro. Isto realízase sobre a base dun rexistro que pode realizarse pola Internet, sempre e cando se utilice un DNIe ou outro certificado que esta normativa defina como documento recoñecido. Ademais, o novo certificado herdaría a fortaleza do certificado sobre a base do cal se fai ese rexistro telemático. "Iso o que permite é a proliferación de prestadores de servizo virtuais", engade, ao tempo que asegura que con este mecanismo se optimizan e se reducen os custos dunha infraestrutura e loxística de servizos de certificación, a parte máis difícil de asumir por parte das empresas prestadoras de servizos de certificación dixital.

Consultado pola implantación actual da certificación dixital, Juan Crespo explica que dende a Administración pública se desenvolveron diversas accións para impulsar o uso dos servizos telemáticos baseados en certificados electrónicos. Neste sentido destaca tres medidas clave: o propio DNIe como elemento de sinatura electrónica dos cidadáns; a Lei 11/2007, do 22 de xuño, que obriga a Administración pública a dotarse dos medios e sistemas electrónicos que posibiliten os cidadáns a exercer o seu dereito a comunicarse coas administracións por medios electrónicos; e a Lei 56/2007, do 28 de decembro, de Medidas de Impulso da Sociedade da Información, coa que se obriga as empresas que prestan servizos básicos aos cidadáns a xestionar os devanditos servizos a través da Internet.

Neste sentido, foi a Adsministración pública a que máis apostou polo desenvolvemento de todos os servizos e usos asociados á certificación dixital, polo que está "plenamente integrado" neste ámbito. Non obstante, no sector privado non se adquiriu aínda o mesmo nivel de implantación.

Percepción e seguridade do DNIe

No referente á percepción do DNIe por parte da cidadanía, o inspector xefe do Corpo Nacional de Policía da área de Informática é tallante: "Non existe un coñecemento demasiado amplo de todo o relacionado con esta tecnoloxía por parte dos cidadáns, a pesar das campañas de formación e sensibilización levabas a cabo pola Policía, o Ministerio de Industria, o INTECO ou o proxecto Red.es entre outros". Así, considera "importante difundir e facerlles chegar aos cidadáns as bondades e a seguridade que ofrece o DNIe ", entre as cales destaca o feito de que este documento asegura a identidade do portador, evitando calquera tipo de suplantación de esta nunha operación.

Nesta liña, hai que recordar que a seguridade da operación que se realiza a través do DNIe radica na entidade que ofrece o servizo, responsable de prestar servizos seguros. Para iso, en colaboración co

Ministerio de Industria, o INTECO, Red.es e o Centro Criptológico Nacional, elaborouse de xeito conxunto unha serie de guías de uso das aplicacións que empregan o DNIe, así como unha serie de perfís de protección. O obxectivo é que as aplicacións que utilizan o DNIe se poidan certificar contra eses perfís de protección, podendo así garantirlles aos cidadáns que as devanditas aplicacións son totalmente seguras. "Que cando asinas algo non hai suplantación do documento que ti estás asinando", matiza.

A este respecto, subliña que dende o Corpo Nacional de Policía non só se certifica como seguro o *chip* do DNIe, senón que, ademais, actualmente se está a proceder a certificar conforme á ISO 27001, o estándar internacional aprobado en 2005 no que se recollen os requisitos para establecer, manter e mellorar un sistema de xestión da seguridade da información. O reto agora é lograr que as aplicacións que fan uso do DNIe estean tamén certificadas, para transmitirlles así aos cidadáns unha sensación e realidade de seguridade a todos os niveis. "Dende o meu punto de vista como cidadán, gustaríame que todas as aplicacións que use sexan certificadas, porque é o único xeito de garantir que estou a facer unha operación segura", recalca Juan Crespo.

Usos do DNIe

O Corpo Nacional de Policía emitiu ata o momento máis de 20 millóns de DNIe, o que supón que máis do 50 por cento da poboación española dispón deste documento (tendo en conta que os menores de 14 anos non teñen obriga de estar identificados a través do DNI). A pesar da gran porcentaxe de poboación que conta con este dispositivo e, aínda que ao emitilo se lle ofrece ao titular documentación informativa sobre os seus usos, aínda existe unha limitación en canto a idade, formación e dispoñibilidade de banda larga á hora de facer un correcto uso do DNIe. Por iso, aínda hoxe en día non se alcanzaron os niveis óptimos de funcionalidade deste documento electrónico.

Neste punto, o inspector xefe do Corpo Nacional de Policía lembra que a sinatura electrónica con DNIe ten consideración de sinatura manuscrita e dálle plena operatividade no ámbito da Internet. Pero a pesar dos avances conseguidos a través deste documento o mundo das novas tecnoloxías é imparable e "sempre estamos en constante evolución", polo que sempre aparece algún detalle que permite mellorar o dispositivo. Así, "actualmente se está a traballar no deseño e construción do próximo *chip* para adaptarse á evolución tecnolóxica, prestándolles especial atención ás normas internacionais e á seguridade", detalla.

Nesta liña, Juan Crespo explica que a liberalización dos comando APDU facilita a proliferación ou xeración de aplicacións, xa que permite que cada organización poida xerarse o seu propio interface de acceso ao DNIe. "É igual de seguro, posto que sempre vai requirir o PIN do cidadán, pero é máis sinxelo posto que se poderán definir o seu propio interface e os comandos de acceso a baixo nivel

dentro das súas aplicacións", sinala. Isto permite, por exemplo, incluír nos caixeiros automáticos dos bancos os accesos ao DNIe sen que iso sexa un proceso de adaptación tecnolóxica custosa para a empresa.

Interoperabilidade no mundo electrónico

Co obxectivo de garantir a súa interoperabilidade o DNIe adaptouse á normativa europea e internacional existente. Para iso, antes de deseñar o proxecto do novo documento electrónico España sumouse a distintos grupos de traballo a nivel europeo, como o proxecto EPOCH, que definía unha serie de normas de interoperabilidade. Dende entón os avances foron moitos e moi diversos, polo que España segue participando noutras iniciativas coas que manterse ao día nesta materia. Así, actualmente España, a través do Ministerio de Política Terrirorial y Administración Pública, participa no proxecto STORK, que persegue a interoperabilidade electrónica na Unión Europa e no que participan organizacións españolas tanto públicas coma privadas. Como exemplo do traballo desenvolvido por España, Juan Crespo explica que precisamente a este grupo se lle enviaron os comandos APDU para que sexan incluídos nun *middleware* común que se está a construír co fin de validar todas as tarxetas de identidade electrónica europeas.

Para garantir a interoperabilidade do DNIe, España tamén traballou a unha escala inferior, pero non por iso menos importante. Así, hai que destacar os acordos formalizados con Portugal para o recoñecemento mutuo dos certificados electrónicos dos documentos de identidade entre ambos os dous países, todo isto coa colaboración do Ministerio de Política Territorial y Administración Pública, que mediante a súa plataforma @firma, valida os certificados dixitais portugueses para o seu uso en España.

Retos de futuro

Tal como recoñece Juan Crespo, a situación económica actual supuxo un freo importante neste tipo de iniciativas tecnolóxicas, xa que se trata de proxectos que requiren un investimento considerable e cuxa rendibilidade non pode medirse a curto prazo. "Hai que adaptar todos os procedementos físicos ao mundo electrónico, e iso require un custo", recoñece. Ademais, o feito de que os proxectos que se realicen deban garantir a súa compatibilidade tecnolóxica no futuro supón un incremento dos custos, o que limita os investimentos nesta materia. "Existen unha serie de custos ocultos que irán aparecendo conforme se materialicen estas necesidades, a nivel de custodia electrónica, por exemplo", avanza.

A pesar da conxuntura económica, os avances realizados en materia de certificación dixital puxeron de manifesto a necesidade de acurtar os prazos de vida do soporte físico para igualalo ao electrónico.

De feito, un paradoxo actual é o feito de que o soporte físico ten unha validez que pode chegar aos dez anos, mentres que a Lei de Sinatura Electrónica establece que o período máximo dun certificado electrónico debe ser de catro anos, o que require unha sincronización da renovación física e a renovación electrónica.

Outro dos retos de futuro pasa pola necesidade de crear un documento de identidade electrónica para os estranxeiros, aos que actualmente non se lles proporciona certificados de identidade nin de sinatura electrónica. Así, neste momento unha persoa de nacionalidade estranxeira debe acudir a unha entidade privada para solicitar un documento deste tipo. O único avance realizado neste sentido materializarase a partir deste verán, cando as tarxetas de identificación de estranxeiros incorporen un *chip* de radiofrecuencia, similar ao do pasaporte electrónico, que permita verificar que non foi manipulada a parte física. Pero este sistema terá única e exclusivamente validez para a identificación presencial, polo que aínda haberá que avanzar ao respecto.

Neste sentido, os proxectos actuais de pasaporte electrónico e a futura tarxeta de identificación electrónica de estranxeiros son "decisións comunitarias, homoxéneas, compatibles e interoperables ao cen por cen dentro da Unión Europea". Ademais, o novo pasaporte electrónico ten unha parte compatible e interoperable co resto dos países que conforman a Organización Internacional de Aviación Civil.

Tamén en materia de servizos asociados á certificación electrónica se presentan novos e importantes retos. "Un reto para a Administración pública é ofrecerlles servizos de calidade aos cidadáns", asegura Juan Crespo, ao tempo que explica que, para o Corpo Nacional de Policía, ofrecer o DNIe non supón soamente expedir o documento e os certificados electrónicos aloxados en este, " senón ofrecer servizos de alta dispoñibilidade, como son as listas de certificados revogados, servizos que lles faciliten aos prestadores de servizos de validación o acceso ás devanditas listas e manter os servidores en liña as 24 horas do día os 7 días da semana".

2.5. FirmaProfesional

Firmaprofesional naceu no ano 2001 como un proxecto de diversos colexios profesionais co fin de actuar con total independencia como Autoridade de Certificación Dixital dos Profesionais.

Firmaprofesional, Sociedade Anónima que inicia a súa actividade en xaneiro de 2002, é un operador global de servizos de certificación e provedor tecnolóxico de seguridade e confianza, ofrecéndolle ao mercado a súa especialización e experiencia, entre outros, nos ámbitos de tecnoloxía, seguridade e normativa legal.

Firmaprofesional, que é unha das empresas pioneiras en España como Autoridade de Certificación, emite certificados dixitais especializados tanto para os profesionais, os seus colexios e colectivos, coma para as empresas e os seus empregados e xera sobre eles unha serie de servizos de valor engadido para o mercado.

Os certificados dixitais de persoa física e persoa xurídica que emite Firmaprofesional son Certificados Recoñecidos, pero para determinados proxectos en ámbitos pechados de usuarios Firmaprofesional tamén comercializa Certificados para Sinatura Electrónica Avanzada.

2.5.1. Entrevista con Santiago Núñez Mella

Santiago Núñez Mella

Responsable de Contas

FirmaProfesional

Santiago Núñez Mella: "Nacemos cun obxectivo claro: cubrir as necesidades dos colexios profesionais en materia de certificación dixital"

O responsable de Contas de Firmaprofesional destaca a vocación dunha entidade que dende 2001 soubo atender de xeito eficiente a demanda dos colectivos profesionais de toda España

A adaptación ás necesidades do cliente, o eficiente sistema de soporte e mantemento e a especialización no ámbito de colexios profesionais son, a xuízo de Núñez Mella, os puntos claves do éxito da empresa

Cando, no ano 2001, bota a andar Firmaprofesional, faino cun obxectivo claro: cubrir as necesidades

dos colexios profesionais, faltos ata o momento dun certificado dixital específico que os identificase como persoas físicas adscritas a un colectivo profesional. Segundo explica o director de Contas de Firmaprofesional, Santiago Núñez Mella, ata entón ningunha Autoridade de Certificación emitía certificados de colexiado, limitábanse a certificados dixitais de persoa física ou a certificados de atributo para colexios profesionais que carecían da suficiente funcionalidade. Núñez Mella déixao claro: "Nacemos cun obxectivo claro: cubrir as necesidades dos colexios profesionais en materia de certificación dixital".

Pero Firmaprofesional non se limita a emitir certificados dixitais para colexios profesionais e vai máis aló, creando autoridades de rexistro nestes colectivos, de xeito que eles mesmos son autónomos para manter todo o ciclo de vida do certificado. Todo este sistema de certificación dixital resulta no ano 2001 "novidoso e moi idóneo para estes colectivos profesionais" e supón deixar en man dos propios colexios profesionais a súa xestión en materia de certificación dixital xa que, tal como apunta Núñez Mella, son eles os que teñen o mellor coñecemento e control do seu colectivo.

Aínda que a andaina de Firmaprofesional se inicia como un proxecto de diversos colexios profesionais co fin de actuar con total independencia como Autoridade de Certificación Dixital dos profesionais e se orienta nun primeiro momento exclusivamente ás necesidades específicas dos profesionais e das entidades que os agrupaban, na actualidade ampliou o seu eido de actuación e ofrece servizos de certificación tanto a corporacións públicas e privadas coma a empresas.

Así explícao o responsable de Contas de Firmaprofesional, quen afirma que, froito da experiencia cos colexios profesionais, se amplía o conxunto de accionistas da empresa con novas entidades como a patronal da pequena e mediana empresa de Cataluña, orientándose Firmaprofesional a servizos máis globais, como consultaría estratéxica ou factura electrónica, entre outros.

Retos de futuro

O futuro da sinatura está clara: "Exportar a experiencia a outros países". Así, o reto fundamental ao que se enfronta Firmaprofesional día a día é seguir implantando e concienciando acerca das bondades do uso do certificado dixital, tanto na Administración pública coma na empresa privada. "É necesario concienciar do beneficio e do aforro de custos, algo do que xa se decataron moitas empresas, aínda que tamén hai outras moitas que non o utilizan", explica Núñez Mella.

"Queremos poder e saber transmitir, facer un eficiente labor de comunicación para que a xente aborde este tipo de proxectos", continúa. Ademais, céntrase nas súas declaracións na importancia que a investigación e os avances tecnolóxicos teñen neste eido concreto, polo que a súa firma aposta por seguir facendo I+D+I para dispoñer de novos produtos e servizos cos que adiantarse á normativa e facilitarlles aos seus clientes todos os trámites posibles con valor engadido.

Produtos e servizos

É necesario diferenciar dous tipos de actuacións dentro de Firmaprofesional, por unha banda diféreancianse os produtos, nos que se inclúen os propios certificados dixitais; a comercialización dos dispositivos onde se almacenan estes certificados de xeito seguro (*tokens*, tarxetas criptográficas...), xa que o 98 por cento dos certificados emitidos van en dispositivos seguros de creación de sinatura; e as plataformas de sinatura. Por outra parte habería que detallar os servizos: de selo de tempo, coñecido como *timestamping*; de validación doutros certificados de balde; e de consultaría e definición de procedementos.

Acerca do valor engadido que lle ofrece Firmaprofesional aos seus produtos e servizos fronte a outras autoridades de certificación dixital, o responsable de Contas da firma teno claro: a adaptación que nós lle facemos ao cliente, adaptamos a solución e a personalizamos en función do cliente. Ademais, estamos especializados en colexios profesionais, traballamos con máis de 80 en toda España". E xunto a estas dúas claves, no seu día a día, non hai que esquecer a "eficiente" axuda que Firmaprofesional lle presta ao cliente en soporte e mantemento, en incidencias funcionalmente básicas pero tecnicamente complexas. De feito, un estudo realizado o pasado ano pola súa empresa revela un alto grao de satisfacción do cliente en materia de atención e servizo.

Uso de certificado dixital

A certificación dixital está estendida dende hai anos nos colexios profesionais de España, con técnicos visadores que utilizan a sinatura electrónica e con colectivos que usan este sistema electrónico para visar, evitando cada vez máis o uso do papel. Ademais, Núñez Mella destaca o feito de que cada vez máis a Administración pública poña a disposición da cidadanía un maior número de servizos telemáticos, co conseguinte avance tecnolóxico e de beneficios para o cidadán.

O uso da certificación dixital é, para Santiago Núñez Mella, un avance porque supón aforro de tempos, de custos e de loxística, pero que ao mesmo tempo ofrece uns niveis de seguridade máis elevados. "A sinatura electrónica non só garante a identidade, senón a integridade, xa que o documento non se modifica dende que a persoa o asinou," detalla. De feito, refírese ao DNIe como un dispositivo seguro que lle facilita ao cidadán a realización de trámites con total seguridade, ao tempo que "crea cultura do uso de certificados dixitais de cara á empresa, vendo os beneficios que leva consigo ofrecer operacións telemáticas". O aspecto negativo deste avance é a escasa información que se lle ofreceu á cidadanía sobre o seu uso o que, unido á falta de lectores de tarxeta para o DNIe, provocou o descoñecemento e desinterese desta tecnoloxía por parte da poboación. "A crise económica tampouco está a axudar a que as empresas se aventuren a acometer novos proxectos para avanzar no uso do DNIe, porque a rendibilidade se vería a medio prazo", apostila.

Neste aspecto, laméntase que nin empresas nin cidadáns sexan conscientes dos beneficios que estes avances en materia de certificación dixital teñen para o seu día a día. "Este proceso de implantación require o seu tempo", recoñece, citando como exemplo o proceso de implantación que tivo no seu día a telefonía móbil. Neste punto, considera Núñez Mella que a Administración pública debería actuar como catalizador dos cambios tecnolóxicos, como por exemplo acontece en Galicia coa factura electrónica, xa que todos os provedores deben integrarse nun sistema para facturar de xeito telemático.

A pesar de encontrarse neste punto de inflexión, o membro de Firmaprofesional subliña que "no ámbito de identidade dixital España está á cabeza, un exemplo é o proxecto do DNIe, pioneiro en Europa". Este liderado supón que agora outros países que comezan nesta aventura dixital teñan a España como referencia, aproveitándose do coñecemento xerado coa experiencia española.

Situación legal

Consultado sobre o marco legal da certificación dixital, o responsable de Contas Santiago Núñez Mella é tallante: "Existen leis pero non todo está suficientemente claro". Tal como explica, ditouse a Lei 59/2003, do 19 de decembro, pero, tendo en conta a progresión dos avances tecnolóxicos, é un marco legal que queda desfasado. "Ás veces hai unha aplicación un tanto laxa da lei para facilitar a introdución desta tecnoloxía", sinala Núñez Mella, quen considera que, ademais, debería existir un réxime sancionador que favorecese a aplicación de esta.

A nivel europeo, dende Firmaprofesional reclámase a necesidade de dispoñer dun órgano intermedio que actúe de enlace entre todos os países e as súas entidades de certificación dixital, unha cuestión na que xa se está a traballar. Ademais, Núñez Mella é firme na súa opinión de considerar España como un exemplo en materia de certificación dixital: "A experiencia que temos en España deberiamos intentar exportala, e canto antes mellor", reafírmase.

Tamén Santiago Núñez Mella aborda os motivos que levan unha Comunidade Autónoma a converterse en entidade de certificación dixital ou prestadora de servizo, algo que, ao seu xuízo non resulta necesario, " senón máis ben é unha ausencia de optimización de recursos". "Deberiamos tender a proxectos máis globais", engade, ao tempo que recorda que crear unha autoridade de certificación "é moi custoso, polo que non vexo lícito que para financiar ese retorno do investimento as entidades de comunidades autónomas compitan en dar servizo a administracións públicas autonómicas ou locais fronte a outros provedores de servizo privados, nin que publiquen concursos públicos que limiten a participación de provedores de servizo privados". Ademais, matiza que, en calquera caso os sistemas deberían ser interoperables aceptando así os certificados de calquera entidade homologada polo Ministerio de Industria.

Certificado dixital: nexo de unión

Para o responsable de Contas de Firmaprofesional, o futuro da certificación dixital pasa por que tanto as entidades públicas como privadas de certificación tendan ao uso do DNIe para evitar ter que acreditar a súa condición de profesional ou asociado, entre outros. Neste punto diferencia, por unha parte, o labor realizado dende a Fábrica Nacional de Moneda y Timbre (FNMT) quen, segundo o seu criterio, "fixo ben o seu traballo", pero aínda así a cidadanía descoñece que a emisión do certificado dixital é gratuíto para o cidadán pero non o é a validación para a entidade pública ou privada, algo que, tal como apunta Núñez Mella, estas entidades non ven con bos ollos.

Por iso, ao seu xuízo, o DNIe desprazará estes certificados, limitarao a existencia da FNMT como autoridade certificadora unicamente para a Administración pública, traballando de xeito exclusivo na emisión de certificados de funcionario, sede electrónica e selo electrónico.

"Entidades públicas e privadas tenderán nun futuro ao uso do DNIe" recalca Santiago Núñez Mella, quen apunta que o uso deste documento se complementará a nivel profesional co certificado profesional, que cubrirá as necesidades de profesionais e asociados. Como exemplo, cita a implantación da telefonía móbil, con dous usos distintos e complementarios: o móbil persoal e o móbil profesional, cada un cos seus fins particulares.

Neste punto entran en valor os servizos prestados por Firmaprofesional que, segundo detalla o responsable de Contas da firma, son economicamente máis competitivos respecto a entidades como a FNMT, "quen debe ter uns custos máis razoables, máis cando se financia con fondos públicos".

2.6. FNMT-CERES

A revolución da tecnoloxía de información, conxuntamente co desenvolvemento da infraestrutura de comunicacións, está a facer cambiar significativamente as relacións entre individuos e organizacións, tanto en España coma en todo o mundo. Estas novas vías de comunicación abren un grande abano de posibilidades, tanto para cidadáns coma para empresas, e permiten comercializar produtos e servizos dun xeito áxil e económico.

En España, as distintas administracións están a apostar decididamente pola Internet como vía de comunicación, creando webs con información de interese público a disposición da cidadanía. Estas iniciativas están a ter unha grande aceptación e repercusión positiva na opinión pública, que está a demandar unha utilización máis xeneralizada da Rede.

Unha das máis ambiciosas destas iniciativas, postas en marcha pola Administración, é o denominado proxecto CERES (certificación ESpañola) que lidera a Fábrica Nacional de Moneda y Timbre, e que en liñas xerais, consiste en establecer unha Entidade Pública de Certificación, que permita autenticar e garantir a confidencialidade das comunicacións entre cidadáns, empresas ou outras institucións e administracións públicas a través das redes abertas de comunicación.

As posibilidades de CERES cobren todas aquelas relacións entre as distintas administracións (Central, Autonómica e Local) e os cidadáns que necesiten ser securizadas en termos de garantía de identidade, confidencialidade e integridade, co obxectivo de que CERES facilite ao máximo as súas relacións a través das novas redes de comunicacións.

O obxectivo principal de CERES é a securización das comunicacións electrónicas coa Administración, sendo un intermediario transparente ao usuario que lles garantirá a cidadáns e Administracións a identidade de ambos os dous partícipes nunha comunicación, así como a confidencialidade e integridade da mensaxe enviada.

Para iso, CERES utiliza técnicas e sistemas criptográficos baseados no que se coñece como sistema de clave pública, con dúas características básicas:

- A identidade do usuario, ao igual que a súa capacidade de sinatura, encóntrase, no caso de máxima seguridade, almacenada nunha tarxeta intelixente, que non pode ser accesible agás polo seu propietario cando introduza o número de identificación persoal, similar á clave dunha tarxeta de crédito. No caso de non utilizar tarxeta, o perfil criptográfico queda almacenado nun ficheiro, sendo necesario tamén un PIN de acceso.
- O sistema é completamente transparente ao usuario, é dicir, non é necesario coñecer ningunha técnica criptográfica para realizar ou verificar unha sinatura elec-

trónica ou cifrar ou descifrar unha mensaxe.

2.6.1. Entrevista con Javier Montes Antona

Javier Montes Antona

Dirección de Sistemas de Información

Xefe de Servizo de Relacións Externas

Departamento CERES

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

Javier Montes Antona: "En certificación electrónica a Fábrica Nacional de Moneda y Timbre pon a seguridade por enriba doutros parámetros"

O xefe de servizo de Relacións Externas do proxecto CERES da Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda aposta polo servizo público como o principal obxectivo da institución en materia de certificación electrónica.

A Fábrica Nacional de Moneda y Timbre (FNMT) ofrécelles aos usuarios unha confianza tradicional avalada polos distintos produtos e servizos que presta a institución dende a súa creación

Co proxecto CERES (certificación ESpañola) España dá un paso máis no uso das novas tecnoloxías e aposta decididamente pola Internet como vía de comunicación entre a Administración e a cidadanía. Liderado pola Fábrica Nacional de Moneda y Timbre (FNMT), o proxecto nace co obxectivo de establecer unha entidade pública de certificación que permita autenticar e garantir a confidencialidade das comunicacións entre cidadáns, empresas ou outras institucións e as administracións públicas a través das redes abertas de comunicación. O xefe de servizo de Relacións Externas do proxecto CERES, Javier Montes Antona, defende esta ambiciosa iniciativa tecnolóxica promovida pola Administración e destaca, como principal característica, a seguridade e confianza que este servizo lles ofrece a todos os seus usuarios.

"A certificación é un tema de confianza e seguridade", sinala Javier Montes, e, neste sentido, a FNMT ofrece a confianza tradicional avalada polos múltiples e distintos produtos e servizos que se ofertan dende hai anos - como os pasaportes, os DNI ou os selos - e a confianza adicional de ter como respaldo o Estado. Ademais, "FNMT ofrece unha seguridade maior que a que pode ofrecer unha empresa privada, que sempre busca os beneficios. Non é que nós busquemos perdas", matiza, " pero poñemos

a seguridade por enriba doutros parámetros".

Outro valor diferencial que ofrece o servizo prestado pola FNMT con respecto a entidades privadas baséase na facilidade para a obtención do certificado dixital, xa que se dispón dunha ampla rede de oficinas de rexistro próximas aos cidadáns onde obter o certificado electrónico Clase 2. Ademais, este certificado pode obterse no estranxeiro a través de embaixadas e consulados. A obtención do certificado electrónico FNMT Clase 2 é gratuíta, e poden solicitala tanto os españois como os estranxeiros residentes en España que dispoñan dun NIE.

A FNMT ten unha parte clave de servizo público, non se pretende rendibilizar cada un dos produtos, senón que se traballa para tratar de expandir ao máximo o uso da sinatura electrónica, tanto na Administración Pública e nas empresas, coma no ámbito nacional e internacional.

Usos do certificado electrónico

Co certificado electrónico expedido pola FNMT pódense realizar todo tipo de trámites pola Internet de xeito que se garante a verdadeira identidade do usuario, ao tempo que permite asinar electronicamente formularios e documentos electrónicos coa mesma validez xurídica que se se asinase con puño e letra o mesmo documento en papel. Deste xeito, o usuario ten a posibilidade de realizar multitude de xestións durante as 24 horas do día, evitando desprazamentos e esperas.

O responsable de Relacións Externas do proxecto CERES destaca que o uso da certificación electrónica está máis estendida na Administración Xeral do Estado, sendo a Axencia Tributaria líder neste uso para a realización da Declaración da Renda. Segundo detalla, hai máis de 100 millóns de trámites telemáticos realizados ante a AEAT con este tipo de certificado. O 98 por cento das declaracións de Renda que foron presentadas a través da Internet utilizaron certificados electrónicos da FNMT. "E ano a ano está crecendo o número de usuarios que utilizan o certificado, e iso é importante". Por outra banda, Javier Montes recoñece que o uso da certificación electrónica tamén está amplamente estendido noutras administracións estatais, como por exemplo a Seguridade Social, especialmente no referido ás consultas sobre vida laboral. "Na Administración Autonómica existen diferentes graos de implantación, aínda que estes últimos anos asistimos a un esforzo moi importante por modernizar e axilizar os trámites telemáticos nalgunhas comunidades autónomas, e mesmo por parte dalgunhas corporacións locais. En último lugar falaría das empresas privadas, que seguen un ritmo bastante máis lento na adopción da sinatura electrónica que as administracións públicas," explica.

Aínda que poida parecer que a certificación electrónica se limita a trámites moi concretos, tal como detalla Javier Montes Antona, todo proceso novo comeza de xeito similar e primeiro se automatizan e modernizan aqueles 4 ou 5 trámites que supoñen o 80 por cento dos servizos prestados aos cidadáns e, posteriormente, automatízanse centos de eles que dan lugar ao 20 por cento residual. Así, coméza-

se con aplicacións como o padrón, nos concellos, ou o cambio de médico e pouco a pouco tratamos de optimizar o resto das prestacións. "Imos avanzando, aínda que quizais non coa velocidade desexada, sobre todo nestes tempos de crise que sempre supoñen un freo nestas cousas", asevera.

Consultado sobre o retorno do investimento realizado en materia de certificación electrónica, o responsable de Relacións Externas do proxecto CERES recoñece que se trata dun retorno "non inmediato", pero que nesta cuestión o Estado tamén se move polo interese de prestar máis e mellores servizos e, así, mídese o retorno noutros parámetros ou valores, como poden ser a seguridade ou os beneficios sociais. "A Administración Pública non mira só a rendibilidade inmediata", recorda Montes Antona, para quen o investimento acabará retornando, "non a curto, senón a longo prazo". Neste aspecto, si considera que a empresa privada se encontra máis limitada porque se move a curto prazo e ten outras opcións distintas á certificación dixital que, aínda que non son tan seguras, ofrecen bos niveis de garantía con custos máis alcanzables, aínda que subliña que si se aprecia que o *e-commerce* está a avanzar moito co uso da factura electrónica.

A FNMT emitiu xa máis de 5 millóns de certificados electrónicos, dos cales 2,5 millóns están activos e vixentes. Ademais, hai preto de 9 millóns de DNIe emitidos. Estas cifras reflicten que hoxe en día existe un público aínda minoritario, que puido comprobar as vantaxes do uso dos certificados electrónicos, como son evitar desprazamentos, as ringleiras innecesarias e a atención continua.

Neste sentido, hai que recoñecer a funcionalidade do DNIe, "porque o levas sempre enriba", se ben se necesita un lector do que non todos os ordenadores dispoñen e isto supón unha barreira que hai que superar, porque non todo o mundo ten acceso ou coñecemento para realizar estas operacións.

Lexislación

En materia de lexislación o membro do proxecto CERES entende que xeralmente as leis foron sempre "un pouco por detrás dos avances tecnolóxicos, aínda que hoxe en día esta cuestión se estabilizou". Neste aspecto destácanse como puntos clave a Lei 59/2003, do 19 de decembro, que equipara a sinatura electrónica coa sinatura manuscrita, e a Lei 11/2007, do 22 de xuño, que obriga a Administración Pública a dotarse dos medios e sistemas electrónicos que lles posibiliten aos cidadáns a exercer o seu dereito a comunicarse coas administracións por medios electrónicos. Defínese así unha nova tipoloxía de certificados electrónicos, como son os de sede electrónica, selo para actuación administrativa automatizada e certificado de empregado público.

Cabe destacar aquí o Real Decreto 1671/2009, polo que se desenvolve parcialmente a citada Lei 11/2007 no ámbito da Administración Xeral do Estado.

Neste sentido, para Javier Montes Antona a actual crise que vivimos supuxo un parón nos avances

nesta materia, xa que de darse outra conxuntura económica a Administración Pública tería dado un salto "máis cuantitativo e cualitativo" na oferta de servizos a través da Internet. Actualmente trátase de cumprir coa lexislación e o que é importante é ter en conta que neste momento calquera cidadán pode esixir que calquera procedemento estea na Internet.

A Lei 59/2003 equipara a sinatura electrónica coa manuscrita tanto no ámbito público como privado. Se ben o uso de certificados electrónicos recoñecidos está máis estendido nos procedementos relacionados coa Administración Pública, a percepción de calidade e seguridade deste sistema por parte dos usuarios particulares pode comprometer as empresas privadas que, co tempo, se queren coidar a súa imaxe e ofrecer servizos máis seguros a través da Internet, rematarán por utilizar este tipo de certificados.

Escenario internacional

Consultado sobre o uso da certificación electrónica a nivel internacional, o responsable de Relacións Externas do Proxecto CERES explica que hai proxectos a nivel europeo e global pero que se están a atopar con diversas dificultades, sobre todo de interoperabilidade, porque hai diferentes sistemas de uso dos certificados, como as certificacións cruzadas, nas que é difícil delimitar as responsabilidades entre as partes. "A data de hoxe en día aínda non se chegou a unha solución global", conclúe.

Así mesmo, Javier Montes Antona explica que en xullo deste ano a Comisión Europea adxudicoulle á FNMT un contrato de servizos PKI (Infraestrutura de Clave Pública). Isto significa que a FNMT é o Provedor de Servizos de Certificación que emitirá os certificados electrónicos dos empregados da Comisión Europea e de 27 Institucións e Axencias da Unión Europea, así como os certificados dos servidores web de estas.

Comunidades autónomas ante a certificación

As comunidades autónomas de País Vasco, Cataluña e Valencia convertéronse en entidades de certificación ou prestadores deste tipo de servizos. Para Montes Antona o feito de converterse en entidade de certificación non se trata dunha cuestión de aforro económico, posto que é máis rendible compartir recursos que desenvolver un servizo propio; nin de compatibilidade ou tecnolóxico, senón que se trata máis ben dun xeito de tratar de defender a propia identidade autonómica a través dunha certificación propia.

"Para min a identidade manifféstase mellor mediante o investimento na mellora dos propios servizos que lles prestas aos teus cidadáns telematicamente", apunta Montes Antona, quen persoalmente cre nun investimento "máis orientado aos servizos que ofrezan máis valor e pensando que hai un camiño

longo de cara a ofrecer o 100 por cento dos servizos ao cidadán "de xeito telemático".

Neste punto, considera que as comunidades autónomas avanzaron de xeito notable en materia de adaptación á Lei 11/2007. "Estamos bastante avanzados, aínda que sería difícil cumprila na súa totalidade, pero levamos un bo camiño", subliñou.

Visión de futuro

O futuro da certificación electrónica pasa, para o responsable de Relacións Externas do Proxecto CERES, na capacidade para mirar cara a Europa e interoperar coa Unión Europea nun primeiro nivel e co resto dos países noutro segundo nivel, levando a cabo macroacordos entre as entidades.

Sobre a perdurabilidade dos provedores de servizos de certificación será a lei da oferta e a demanda a que decida cales continuarán e cales desaparecerán, cuxos certificados terá que asumir por obriga o Ministerio de Industria. "Posiblemente os pequenos provedores desaparecerán ou deberán facer alianzas. O propio mercado é o que dirá", apostila Montes Antona.

2.7. INTECO, Instituto Nacional de Tecnoloxías da Comunicación

O **Instituto Nacional de Tecnoloxías da Comunicación, S.A. (INTECO)** é unha sociedade mercantil estatal, con sede en León (España), adscrita ao Ministerio de Industria, Turismo y Comercio a través da Secretaría de Estado de Telecomunicaciones e para a Sociedade da Información. Está participada ao 100% pola Entidade Pública Empresarial red.es.

INTECO créase, logo de autorización do Consello de Ministros na súa reunión do 27 de xaneiro de 2006, para responder a un dobre obxectivo: por unha banda, contribuír á converxencia de España con Europa no ámbito da Sociedade da Información, desenvolvendo proxectos innovadores no ámbito da tecnoloxía da comunicación e, por outra, promover o desenvolvemento rexional, enraizando en León un proxecto con vocación global.

INTECO é un centro de desenvolvemento de carácter innovador e de interese público de ámbito nacional que se orienta á achega de valor, á industria e aos usuarios, e á difusión das novas Tecnoloxías da Información e a Comunicación (TIC) en España, en clara sintonía con Europa.

O seu obxectivo fundamental é servir como instrumento para desenvolver a Sociedade da Información, con actividades propias no ámbito da innovación e o desenvolvemento de proxectos asociados ás TIC, baseándose en tres piares fundamentais: a investigación aplicada, a prestación de servizos e a formación.

Por outra banda, INTECO aparece expresamente constituída como medio propio e servizo técnico da Administración Xeral do Estado, co que está obrigada a realizar os traballos que lle encomenden os diferentes departamentos ministeriais da Administración Xeral do Estado nas materias obxecto das súas funcións dun xeito áxil e eficaz a través da figura das encomendas de xestión.

A misión de INTECO é achegarlles valor e innovación aos cidadáns, ás PEMES, ás administracións públicas e ao sector das tecnoloxías da información, a través do desenvolvemento de proxectos que contribúan a reforzar a confianza nos servizos da Sociedade da Información en España, promovendo ademais unha liña de participación internacional.

A visión de INTECO é conseguir os seus obxectivos mediante:

- O compromiso de profesionais altamente cualificados, comprometidos cos seus proxectos e capaces de xerar valor e innovación continuamente.
- A dinamización do sector TIC, xerando novos negocios e oportunidades para clientes, provedores e profesionais.
- A igualdade de oportunidades para todo o tecido empresarial español, especialmente a PEME, actuando como subministración de último recurso en materia de

innovación TIC aló onde sexa necesario.

- O soporte aos cidadáns, que son a clave para que o desenvolvemento das novas tecnoloxías teña un impacto social positivo.

2.7.1. Entrevista con Marcos Gómez Hidalgo

Marcos Gómez Hidalgo

Subdirector Programas

Dirección de Operacións

INTECO: Instituto Nacional de Tecnologias de la Comunicacion

INTECO aposta pola formación e a sensibilización como claves para achegarlle as aplicacións da certificación dixital, entre elas a sinatura electrónica, á cidadanía

O subdirector de Programas do Instituto Nacional de Tecnologías de la Comunicación, Marcos Gómez Hidalgo, subliña que é na Administración pública e nas empresas onde está máis estendido o uso desta nova tecnoloxía

Para Gómez Hidalgo é necesario que os usuarios coñezan que ao crear/utilizar servizos con certificados dixitais (en particular con sinatura dixital) se producen aforros de custos e tempo e de eficiencia fronte aos mesmos servizos sen esta tecnoloxía.

Divulgar o uso e as vantaxes das aplicacións dos certificados dixitais, principalmente a sinatura electrónica, entre a cidadanía e superar as dificultades, tanto técnicas coma de formación, nesta materia son os retos que se formula o Instituto Nacional de Tecnologías da Comunicación (INTECO) de cara ao futuro. Hoxe en día a complexidade técnica, o descoñecemento xeral da súa utilidade e a falta de confianza nesta nova tecnoloxía son as principais dificultades coas que o cidadán de a pé se encontra á hora de introducirse no uso da sinatura electrónica. Así explícao o subdirector de Programas de INTECO, Marcos Gómez Hidalgo, quen formula como obxectivo superar estas barreiras, difundir entre a cidadanía as vantaxes que os certificados dixitais poden ofrecerlles, tanto en aforro de custos coma de tempo, e ao mesmo tempo favorecer o desenvolvemento de novos servizos, públicos e privados, nos que se poida operar con confianza, con certificados dixitais.

Baixo o nome de INTECO, funciona dende 2006 unha entidade de carácter público, dependente do Ministerio de Industria, Turismo y Comercio, que ten, un dobre obxectivo: contribuír á converxencia de España con Europa no campo da Sociedade da Información a través de proxectos innovadores en

tecnoloxía da comunicación; e, por outra banda, promover o desenvolvemento rexional. Así, o centro serve de instrumento para desenvolver a Sociedade da Información en España, en sintonía con Europa, con actividades propias no ámbito da innovación e o desenvolvemento de proxectos asociados ás TIC, baseándose en tres puntos clave: a investigación aplicada, a prestación de servizos e a formación.

Dende a súa creación INTECO traballa en ámbitos estreitamente relacionados coa sinatura electrónica, tanto no referente a concienciación e sensibilización, como co apoio a desenvolvedores ou o soporte a usuarios e PEMES. A difusión do DNI electrónico é un dos campos básicos de actuación da entidade, que tamén ofrece servizos de consultaría en clientes á Administración pública.

Uso dos certificados dixitais

Na actualidade, o uso da certificación dixital está máis estendido no ámbito da Administración pública, encargada tamén de impulsar estas novas tecnoloxías, mentres que na empresa se emprega principalmente para facturación electrónica ou en iniciativas concretas de certos sectores, como a banca. Facturación electrónica e contratación electrónica son os sectores onde a certificación dixital ten maior promoción. Pola contra, a cidadanía segue descolgada do tren dixital e, aínda que os trámites coa Axencia Tributaria e o DNI electrónico son os usos máis difundidos, distan aínda moito dos niveis desexados. Por isto, o responsable de Programas de INTECO considera fundamental difundir as vantaxes do uso dos certificados dixitais entre as empresas, cidadáns e administracións públicas. Coa Administración electrónica optimízanse custos e tempo, simplifícanse os procesos e aténdese o cidadán dun xeito máis eficiente e seguro, tal como explica Marcos Gómez Hidalgo. Pola súa banda, o cidadán obtén como principal beneficio unha flexibilidade de horarios e ubicuidade, ao tempo que ve reforzada a súa confianza no prestador do servizo.

Sobre a percepción de seguridade que ofrece a sinatura dixital para o cidadán, o subdirector de Programas de INTECO considera que os usuarios critican máis as dificultades técnicas á hora de aplicar os certificados dixitais que a seguridade dos mecanismos da sinatura. Ademais, moitos usuarios demandan unha separación entre o uso particular e o uso profesional dos certificados dixitais. Gómez Hidalgo subliña a necesidade de atallar esta situación de descoñecemento sobre a sinatura dixital a través de iniciativas de formación, concienciación e sensibilización.

Lexislación

A lexislación española actual é "suficiente, clara e completa" en materia de regulación de certificación dixital e sinatura electrónica xa que, ademais a normativa propia, se traspón a Directiva europea en canto a tipoloxía, características e tipos de uso. Nesta liña Marcos Gómez Hidalgo destaca que Espa-

ña é, co DNI electrónico "unha potencia de primeira orde en certificados dixitais", unha situación de liderado que é recoñecida en Europa.

Consultado sobre a compatibilidade lexislativa da certificación dixital nos diferentes países, o subdirector de Programas de INTECO explica que a nivel europeo a propia Directiva 1999/93/CE do Parlamento Europeo e do Consello, do 13 de decembro de 1999, establece xa un marco comunitario para a sinatura electrónica. Esta normativa propicia un marco lexislativo común nos países europeos, mentres que a nivel internacional aínda "queda un longo camiño por percorrer en canto a interoperabilidade", ao tempo que as diferenzas terminolóxicas poden dar lugar a confusións entre individuos procedentes de distintos países ou en contratos internacionais.

Autonomías e certificación dixital

En relación ao papel que xogan as comunidades autónomas como prestadoras de servizos de certificación dixital, Marcos Gómez Hidalgo considera que este tipo de proxectos ofrécenlles o valor engadido de independencia ás propias comunidades, ao tempo que poñen a disposición do usuario servizos que permiten un aumento de confianza con maior eficiencia e trámites máis simplificados. Pola contra, estas iniciativas propias poden repercutir no prezo dos servizos prestados, xa que requiren un investimento por parte das comunidades autónomas, e, eventualmente, pódense ocasionar atrasos se fose necesario contactar con outra entidade para comprobar a validez de certificados externos.

Aínda que, tal como sinala Gómez Hidalgo, resulta difícil medir o retorno dos investimentos que as comunidades autónomas realizan nestes proxectos propios, debe valorarse que as iniciativas autonómicas, ademais de erixirse en referentes para as empresas, poden aproveitarse para consolidar a posición de España en materia de certificación dixital, en particular co uso do DNI electrónico, pioneiro no seu eido.

Futuro do certificado dixital

O futuro presenta grandes retos a superar no campo da certificación dixital. Ademais dos avances propiamente tecnolóxicos e a difusión a nivel usuario, formúlase como convivirán a longo prazo as entidades de certificación públicas e privadas. Neste aspecto, o subdirector de Programas de INTECO teno claro: "cumprindo a lexislación poden convivir ambos os dous tipos de entidades, cada unha terá o seu ámbito de aplicación", xa que a propia normativa establece obrigas e responsabilidades dos prestadores de servizos de certificación e os requisitos para a súa acreditación como tales. Ademais deste feito, considera clave a especialización de cada entidade nun eido concreto, así como a xeración de servizos de valor engadido e a adaptación de produto/servizo e custo. Para Gómez Hidalgo mesmo é necesaria a coexistencia de redes de autoridades nacionais ou sectoriais, interrelacionadas entre si

e con servizos propios a usuarios dos seus respectivos ámbitos de actuación.

Por outra banda, Marcos Gómez Hidalgo aborda tamén os principais retos da sinatura electrónica tanto en España coma en Europa a longo prazo. Neste sentido considera que un aspecto fundamental é traballar na difusión e formación desta tecnoloxía a todos os niveis: usuarios, empresas, desenvolvedores e administracións, ao que deberá unirse unha regulación lexislativa axeitada e común a toda a área de aplicación.

Ademais, Gómez Hidalgo considera necesario avanzar na creación de Autoridades de Certificación Pública gratuítas que ofrezan os servizos básicos de emisión de certificados persoais, de empresa e de facturación, validación e selado de tempo, entre outros, asociados aos correspondentes servizos de mantemento; e na conformación dun estándar que regule o uso da sinatura electrónica na Administración pública, abordando cuestións como a funcionalidade, aspectos visuais identificativos ou tratamento de documentos asinados. A posta en marcha destes proxectos de futuro supoñería, segundo Gómez Hidalgo, unha serie de oportunidades de negocio interesantes a determinar.

E ante os retos de futuro da certificación dixital o Instituto Nacional de Tecnologías de la Comunicación non pode quedar indiferente. Así, entre as súas principais apostas a longo prazo INTECO márcase como meta avanzar en materia de concienciación e sensibilización a través de programas formativos; colaborar coa Administración pública en proxectos de sinatura electrónica; apoiar o desenvolvemento e a certificación de aplicacións de sinatura con DNI electrónico; e dar soporte á liberalización de aplicacións de software de validación e sinatura electrónica, entre outras cuestións. En xeral, o organismo público traballará en todas aquelas propostas que contribúan a xerar confianza no uso dos servizos da Sociedade da Información, unha clara aposta polas novas tecnoloxías ao servizo da sociedade.

2.8. IZENPE, ZIURTAPEN ETA ZERBITZU ENPRESA

Izenpe S.A., Ziurtapen eta Zerbitzu Enpresa/Empresa de Certificación e Servizos é unha Sociedade Anónima constituída en 2002 e supón un proxecto impulsado polo Goberno Vasco e as Deputacións Forais, creado a través das súas diferentes sociedades informáticas:

- EJIE (Eusko Jaurlaritzaren Informatika Elkartea/Sociedade Informática do Goberno vasco): é unha empresa pública do Goberno Vasco que contribúe, mediante a prestación de servizos informáticos, a conseguir unha Administración Pública Vasca moderna e eficiente.
- LANTIK S.A.: é unha sociedade de carácter unipersoal, participada exclusivamente pola Deputación Foral de Bizkaia, que foi constituída no ano 1981 coa finalidade de prover a Institución foral, aos organismos e institucións que dependen de esta e aos concellos de Bizkaia de sistemas de información, encargándose, igualmente, da explotación de estes e da prestación de todo tipo de servizos anexos.
- IZFE S.A. (Informatika Zerbitzuen Foru Elkartea/Sociedade Foral de Servizos Informáticos): ten por obxecto a prestación de servizos informáticos que garantan a consecución da liña estratéxica dos sistemas de información da Deputación Foral de Gipuzkoa no ámbito das tecnoloxías da información e as comunicacións.
- CCASA S.A.: ten por obxecto prestar os servizos que garantan a consecución da visión estratéxica dos sistemas de información da Deputación Foral de Álava no ámbito das tecnoloxías da información e comunicacións.

Os obxectivos xerais de Izenpe son os seguintes:

- O fomento do uso e potenciación do desenvolvemento do Goberno electrónico sobre redes de telecomunicacións coas necesarias garantías de seguridade, confidencialidade, autenticidade e irrevogabilidade das transaccións.
- A prestación, no ámbito das institucións que integran o sector público vasco, de servizos de seguridade, técnicos e administrativos, nas comunicacións a través de técnicas e medios electrónicos, informáticos e telemáticos.
- A expedición, fabricación e subministración dos títulos ou certificados de usuario ou soportes en tarxeta necesarios para persoas ou entidades públicas ou privadas.
- A expedición, fabricación e subministración dos títulos ou certificados de servidor.
- Servizos de Consultaría relacionados coa promoción do goberno electrónico.

2.8.1. Entrevista con Eduardo Portero Delgado

Eduardo Portero Delgado

Director Xeral

Izenpe S.A., Ziurtapen eta Zerbitzu Enpresa/Empresa de Certificación e Servizos.

Eduardo Portero Delgado: "As funcións de Izenpe van moito máis aló de ser un simple prestador de servizos de certificación dixital; agora o noso obxectivo é definir procesos de Administración electrónica"

Para o director xeral de Izenpe, hoxe en día unha Comunidade Autónoma non é só un terceiro de confianza como emisor de certificados dixitais, senón que pode ofrecer novos servizos e situarse á vangarda da e-Administración.

Izenpe é un dos dous únicos provedores mundiais de certificados de servidor seguro SSL con SV, un documento con grande aplicación e demanda na actualidade

Nun marco nacional no que nos últimos anos naceron novas necesidades en materia tecnolóxica, a certificación dixital convértese nun mercado en desenvolvemento. Á creación de organismos a nivel estatal, públicos e privados, prestadores de servizos de certificación dixital, uníronse tamén as iniciativas das comunidades autónomas, dispostas a non perder o tren do progreso tecnolóxico e a dispoñer de autoridades propias, diferentes e adaptadas á súa realidade. Neste marco constitúese no ano 2002 Ziurtapen eta Zerbitzu Enpresa - Empresa de certificación e servizos Izenpe S.A., unha Sociedade Anónima impulsada polo Goberno Vasco e as Deputacións Forais. O seu director xeral, Eduardo Portero Delgado, explica os motivos da súa creación como unha decisión política, "porque ter un prestador de servizos de certificación dixital é caro se se quere que sexa realmente operativo". Pero afirma que, oito anos despois da súa posta en marcha, as funcións de Izenpe "van moito máis aló de ser un simple prestador de servizos de certificación dixital". "Todo o relacionado coa emisión de certificados funciona ben e de xeito automático", explica, "agora o obxectivo é a definición de procesos de administración electrónica".

Para Eduardo Portero Delgado a creación de autoridades de certificación dixital propias nas comunidades autónomas está xustificado porque estas poden cumprir outra serie de calidades. "Hoxe en día unha Comunidade Autónoma non é só un terceiro de confianza ou un simple validador que dá crédito e fe, senón que pode ofrecer unha cantidade de servizos, ao tempo que debe ser a vangarda da Administración electrónica", apunta. Neste sentido, destaca que, na actualidade, Izenpe se encontra á vangarda no desenvolvemento de servizos de consultaría e de estudos para a Dirección de Innovación

e Administración Electrónica do Goberno Vasco.

Produtos e servizos

Segundo explica o director xeral de Izenpe, a maior parte dos seus clientes sitúase no sector público, concellos, deputacións e o Goberno Vasco; mentres que os clientes da empresa privada demandan produtos tecnolóxicos e traballos de consultaría. Neste punto, Portero Delgado destaca o feito de que, en certificación dixital, Izenpe é unha das dúas únicas entidades en todo o mundo que proporcionan certificados de servidor seguro SSL con SV, un certificado con grande aplicación debido á demanda cada vez maior de seguridade nos ámbitos da Internet.

En xeral, os obxectivos de Izenpe pasan por fomentar o uso e o desenvolvemento do Goberno electrónico sobre redes de telecomunicacións coas necesarias garantías de seguridade, confidencialidade, autenticidade e irrevogabilidade das transaccións. Así, traballa na prestación, no ámbito das institucións que integran o sector público vasco, de servizos de seguridade, técnicos e administrativos, nas comunicacións a través de técnicas e medios electrónicos, informáticos e telemáticos. Os principais documentos que emite son certificados dixitais de usuario ou soportes en tarxeta para cidadáns e para entidades, públicas ou privadas; así como certificados corporativos, que son certificados privados para as persoas dunha empresa. Izenpe tamén presta servizos de consultaría relacionados coa promoción do Goberno electrónico. Ademais, segundo sinala o director xeral da entidade, na súa estratexia inclúese seguir ampliando o número de certificados en función dos proxectos de Administración electrónica que xurdan e en función da propia demanda.

No referente a produtos, o máis demandado é a plataforma de servizos de sinatura integrados ZAIN, tal como apunta Portero Delgado. Ademais, Izenpe ofrece outros produtos, como son o servizo de constancia da publicación para a sinatura electrónica; e o Lotura@, un *broker* de identidades ou axente mediador, que funciona de tal maneira que dúas entidades que "compren" o produto dispoñen dun terceiro de confianza (Izenpe), o que lles permite intercambiar determinados datos. Actualmente este sistema utilízase na Deputación foral de Gipuzkoa para conectar as aplicacións de tráfico das policías locais co Ministerio del Interior.

Neste punto, o responsable de Izenpe destaca que o proxecto máis importante de Izenpe é a tarxeta ONA, que supuxo a principal liña de negocio do organismo. Segundo os datos que manexa, actualmente hai aproximadamente 250.000 tarxetas ONA emitidas, un documento que funciona como "unha tarxeta sanitaria para usos cidadáns". A ONA ten asociados dous tipos de servizos: electrónicos e eléctricos. O uso fundamental desta tarxeta é o sanitario e só unha porcentaxe mínima de cidadáns utilizou esta tarxeta para realizar trámites telemáticos. "O grao de empregabilidade da tarxeta ONA, cuxo custo foi moi elevado, é aínda moi baixo -en torno ao 3 por cento-, pero cun grao de satisfacción

moi alto", lamenta Eduardo Portero Delgado. Isto débese, segundo apunta, a que moitos concellos non teñen realizados os desenvolvementos necesarios para realizar trámites electronicamente, o que limita o uso dos dispositivos. E o futuro preséntase difícil para esta tarxeta, xa que o Parlamento Vasco aprobou unha Proposición Non de Lei na que pon fin ao devandito proxecto o próximo 31 de decembro, o que significa que Izenpe non emitirá máis tarxetas ONA, aínda que si está obrigado a custodiar a documentación durante 15 anos, a manter o certificado electrónico vivo durante 4 anos e a operar cos servizos asociados ao plástico durante 10 anos.

Converxencia de dispositivos

O futuro da certificación dixital pasa por unificar dispositivos e definir usos e funcións. Así o expón o director xeral de Izenpe, quen considera que se realmente se quere converter o cidadán nun cidadán dixital é necesario realizar unha converxencia de dispositivos, é dicir, unificar todos os dispositivos electrónicos nun só, manexable e comprensible. "Que os cidadáns vexan que a e-Administración é unha realidade, que é vantaxosa e que lles vai proporcionar mellores relacións coa Administración depende de que haxa unha tendencia real á unificación dos dispositivos electrónicos", formula Portero Delgado.

A xuízo de Eduardo Portero Delgado, é necesario reformularse para que vale a sinatura electrónica e en que ámbitos ten sentido a súa utilización, para o que a Administración Pública debe facer esforzos no despregamento de aplicacións e desenvolvemento de tarxetas como instrumentos para o uso destas aplicacións. "Ata agora poñíase por diante o despregamento de tarxetas antes que o desenvolvemento dos sistemas de información que as ían utilizar", apunta, unha situación que debe cambiar.

Ademais, neste punto, Portero Delgado fai referencia aos novos usos de futuro que ofrecen a biometría, cuxo uso complementario se asocia hoxe en día á sinatura electrónica para aqueles ámbitos "moi delicados".

Normativa vasca

O director xeral de Izenpe refírese tamén á normativa legal na que se enmarca a certificación dixital. Neste sentido, recorda que o Goberno Vasco dispón do Decreto de uso de medios electrónicos, informáticos e telemáticos nos procedementos do Goberno Vasco, unha normativa propia da Comunidade Autónoma en canto á admisión de medios telemáticos na que se establecen os escenarios e condicións técnicas que deben ter os prestadores de certificación para que os seus documentos sexan válidos no ámbito da Comunidade. Deste xeito, calquera autoridade de certificación dixital que desexe operar no País Vasco debe homologarse segundo os requisitos establecidos neste decreto.

Sobre este decreto, Eduardo Portero Delgado recoñece que, aínda que o decreto "é o envoltorio que lle permitiu a Izenpe dobregar o resto de prestadores de servizos de certificación dixital para admitilos ou non, a tendencia é que nun futuro inmediato haxa a obriga a que todos os prestadores no marco europeo se admitan entre eles". Así, apunta a que se tenderá "cara á conxunción de sistemas tecnolóxicos e informáticos" e móstrase convencido de que "haberá un marco europeo de homologación único". En concreto, Porteiro Delgado explica que actualmente se está a discutir sobre como liberar as políticas en materia de certificación dixital (de feito, a Unión Europea traballa xa na definición das políticas de certificados en todo o seu territorio) xa que, aínda agora, existen certificados con políticas moi restritivas, o que provoca que nalgúns casos unha persoa dispoña de varios certificados. Ao seu xuízo, esta situación tamén determina a necesidade, antes apuntada, de que funcione un organismo de carácter supranacional que realice as validacións de identidade.

Lexislación xeral

Máis aló da normativa propia vasca en materia de certificación dixital, o máximo responsable de Izenpe aborda tamén a situación legal a nivel estatal. Ao tempo que recoñece que gran parte do despregamento da Administración electrónica se fixo "a golpe de lei", para el a Lei 11/2007, do 22 de xuño, é "boa, porque é flexible", aínda que, ao seu xuízo, peca de incluír o condicionante da dispoñibilidade orzamentaria, algo que limita o seu desenvolvemento e aplicación práctica.

"A lei xa é suficientemente ampla, non son necesarias novas coberturas legais, o necesario é a vontade ampla, clara e concisa por parte da Administración Pública", explica Portero Delgado, quen detalla que esta vontade debe basearse en explicarlle claramente ao cidadán que é o que pode facer dun xeito sinxelo e claro. Ademais, incide na importancia de elaborar aplicacións que garantan que calquera usuario poderá operar utilizando o ámbito que desexe, é dicir, que se garanta o principio de interoperabilidade e de neutralidade tecnolóxica.

Neste punto, Porteiro Delgado insiste de novo na necesidade de camiñar cara a unha normativa común, xa que considera que un exceso de leis e regulamentacións propias da Administración electrónica -a nivel de concellos, comunidades autónomas, etcétera -pode provocar inseguridade xurídica. “Hai que evitar o desexo de orixinalidade das administracións públicas en canto á lexislación arredor da e-Administración ", conclúe.

A xeito de apuntamento, Eduardo Portero Delgado destaca que Avilés é o concello de España con maior desenvolvemento da Administración electrónica, pero que a maior parte dos trámites se realizan simplemente con nome de usuario e *password*, o que ofrece un baixo grao de seguridade.

Usos da certificación dixital

"Os cidadáns que utilizan a sinatura electrónica é porque teñen claro o seu valor de seguridade", apunta tallante o director xeral de Izenpe, "outra cousa é que o vexan como algo eficaz", engade. Para Eduardo Portero Delgado a cidadanía en xeral ten claro que a sinatura electrónica é un sistema seguro, pero aínda non viron nin a súa utilidade nin a súa eficacia. De feito, segundo detalla, varios estudos apuntan a que a satisfacción dos cidadáns ante o uso de tarxetas intelixentes estaría relacionada con incluír en estas medios de pagamento e medios para o acceso ao transporte público. En todo caso, para Portero Delgado isto é un exemplo da demanda que existe entre a poboación para dispoñer dunha soa tarxeta con todos os usos posibles: o que se coñece como converxencia dixital.

No caso concreto do País Vasco, onde as deputacións son as encargadas de recadar os tributos, o principal uso da sinatura electrónica rexístrase na facturación electrónica. Para iso Izenpe desenvolveu un produto a instancia das propias deputacións, que vían a necesidade de dispoñer dun sistema de facturación electrónica. Ademais, o mesmo organismo público de certificación dixital traballa de xeito habitual con factura electrónica e intenta que todos os seus provedores facturen a través deste sistema.

Retos de futuro

Consultado sobre a convivencia futura das entidades de certificación públicas e privadas o responsable de Izenpe resolve: "Todos os prestadores de servizos de certificación comparten un espazo común, e a competencia e a competitividade son boas". Ademais, engade, "a colaboración actual de Izenpe é moi boa con todos os prestadores de servizos existentes e así debe ser, debido á importancia de todos os temas relacionados co ámbito da certificación".

Nesta liña, para Eduardo Portero Delgado, o máis lóxico será que nun escenario próximo exista unha política común de identificación dos nacionais, é dicir, que Europa cree unha autoridade común en materia de identificación dixital. Ao seu parecer, ao igual que se poden nomear cinco aspectos comúns que identifican fisicamente a todos os cidadáns europeos, se deberá definir unha serie de aspectos que os definen electronicamente, o que levará a crear un sistema común de identificación.

Sobre o futuro da sinatura electrónica, para Portero Delgado, o éxito do desenvolvemento e do uso deste tipo de certificado dixital virá marcado pola existencia dun validador a nivel supranacional, xunto coa aplicación de elementos biométricos asociados e complementados á sinatura dixital para ámbitos delicados. Ademais, móstrase convencido de que serán o propio mercado e os usuarios os que marcarán tendencia en todas as solucións e retos futuros neste eido. Así, pon como exemplo o feito de que na actualidade "hai usuarios e ámbitos que piden cada vez máis seguridade na Rede, polo que é necesario dar un determinado grao de fiabilidade", o que lles obriga a empresas e institucións a traballar nesta área. Así, demandas coma esta trasladaranse a todos os eidos de uso e desenvolvemen-

to das novas tecnoloxías.

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

A Secretaría Xeral de Modernización e Innovación Tecnolóxica configúrase como o órgano superior da Administración autonómica ao que lle corresponde o impulso, asesoramento técnico e apoio en materia de tecnoloxías da información e as comunicacións e a súa aplicación para a modernización, innovación e desenvolvemento tecnolóxico de Galicia.

Este departamento depende directamente do presidente da Xunta e nace con vocación de apoiar e darlles servizo ás diferentes consellarías, buscando a calidade, racionalización das actuacións e a mellora da eficiencia na xestión das TIC.

A súa creación supón a constatación de que as tecnoloxías da información e as comunicacións (TIC) constitúen un instrumento de alto nivel estratéxico polo seu potencial para impulsar a modernización da Administración pública, así como a súa capacidade para impulsar e sustentar o desenvolvemento social e económico de Galicia.

Para a consecución dos seus obxectivos, que non son outros que os expostos no programa e o discurso de investidura do presidente, é imprescindible a colaboración de todos os departamentos e organismos da Xunta.

A Secretaría Xeral de Modernización e Innovación Tecnolóxica debe asumir a evolución permanente das TIC da Xunta para mellorar a eficiencia e achegarlle a Administración ao cidadán e liderar a incorporación plena da sociedade galega ao mundo das TIC.

Isto tradúcese nos seguintes obxectivos:

- Promover un avance significativo de Galicia no marco da Sociedade da Información.
- Ordenar e homoxeneizar as actuacións en materia de TIC de toda a Administración galega (todos avanzando na mesma dirección), garantindo a seguridade da información e a interoperabilidade dos sistemas.
- Extraer o máximo aproveitamento das posibilidades das TIC como dinamizador económico, elemento clave de desenvolvemento sostible e xerador de aforros.
- Adaptar a Administración galega ás demandas sociais e os requirimentos legais (Lei de acceso electrónico dos cidadáns aos servizos públicos) en canto á 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: "A implantación da sinatura electrónica permitiranos avanzar cara unha Galicia 2.0"

A secretaria xeral de Modernización e Innovación Tecnolóxica da Xunta aposta por abordar de xeito integral a acreditación dixital de todas as persoas que interveñen no proceso electrónico

"O crecemento experimentado polo DNI electrónico en Galicia no último ano foi dun 47,7%"

Para a Secretaria Xeral de Modernización e Innovación Tecnolóxica da Xunta de Galicia, Mar Pereira, na medida na que a relación dos cidadáns e a Administración avanza cara ao contexto dixital é imprescindible asegurar que este tránsito se fai xerando un ámbito de confianza na aplicación das tecnoloxías. Xa a propia Lei 11/2007 establece que "o tránsito do procedemento en papel ao emprego das novas tecnoloxías non favoreza un menoscabo das garantías".

"O desenvolvemento da Administración electrónica na Administración pública de Galicia esixe abordar de xeito integral a acreditación dixital de todas as persoas que interveñen no proceso electrónico", asegura Mar Pereira. Por iso un dos eixes de actuación do plan de modernización é facilitar a todos os seus traballadores dos medios que os acrediten dixitalmente e os habiliten coas capacidades de sinatura electrónica necesarias para o desempeño das súas funcións.

Neste sentido están en marcha unha serie de medidas, entre as que cabe destacar a adxudicación do servizo de certificación dixital da Fábrica Nacional de Moneda y Timbre e o proxecto de acreditación dixital do empregado público.

"O recentemente publicado decreto de administración electrónica da Xunta de Galicia, Decreto 198/2010, do 2 de decembro, polo que se regula o desenvolvemento da Administración electrónica na Xunta de Galicia e nas entidades dela dependentes, prevé o marco xeral de aplicación desta acreditación e a elaboración das normas técnicas para o seu desenvolvemento", lembra a secretaria xeral.

Neste mesmo ámbito formúlase ademais a necesidade de avanzar a un maior nivel de uso do DNI electrónico, como instrumento de acreditación dixital do cidadán, polo que os servizos que se ofrecen por parte das administracións deben estar adaptados á súa utilización.

Por outra parte, o desenvolvemento da eAdministración no ámbito dos concellos é un eixe fundamental para a prestación dos servizos públicos en iguais condicións de calidade a todos os cidadáns e empresas independentemente do seu lugar de residencia. Neste sentido e para facilitarlle este desenvolvemento ás administracións locais, e a outras entidades, o contrato asinado coa FNMT prevé a adhesión ao consumo destes servizos da administración local e outros entes da comunidade autónoma sen custo para elas.

Este proceso deberá ir acompañado dunha formación específica dos coñecementos que permitan aos empregados públicos da Administración galega o máximo aproveitamento dos medios postos á súa disposición.

"Non cabe dúbida que nos últimos anos se produciu un avance considerable na extensión do uso da certificación dixital _subliña a secretaria xeral de Modernización e Innovación Tecnolóxica_ e xa non só grazas á oferta de servizos públicos por parte das Administracións Públicas senón tamén grazas á progresiva dispoñibilidade do DNIe por parte dos cidadáns".

"Atendendo a estes dous factores cremos que, neste momento, son as Administracións Públicas as que permiten un uso máis estendido da certificación dixital. Galicia presenta bos resultados no uso dos servizos da eAdministración por parte da cidadanía. No ano 2010, o 51,7% da poboación galega que utilizou Internet obtivo información de páxinas web da administración, superando á media estatal en 5,3 puntos porcentuais. Un 20,3% enviou formularios cubertos a través de Internet (2,6 puntos por enriba da media estatal)", asegura Mar Pereira.

Estes datos sitúan a Galicia como a terceira comunidade autónoma con maior uso da Administración electrónica para obter información das páxinas web e a quinta comunidade en descargar e cubrir formularios oficiais.

Ademáis, un 35% dos cidadáns de Galicia, entre 16 e 74 anos, xa dispoñen do DNI electrónico, 7,5 puntos máis cá media estatal, e un 8% dispón doutros certificados de sinatura recoñecidos. O crecemento experimentado polo DNI electrónico en Galicia no último ano foi dun 47,7%.

"Estes datos indican que temos unha boa base para afrontar os cambios e os futuros retos da Sociedade da Información. Dende o Goberno galego e as distintas administracións debemos impulsar o uso e aproveitamento das TIC e fomentar que o cidadán desenvolva unha cultura dixital e adquira seguridade e confianza no seu uso", afirma a titular da Secretaría Xeral de Modernización e Innovación Tecnolóxica.

É unha das liñas de traballo da Axenda Dixital 2014.gal, a estratexia tecnolóxica global da Xunta, que considera a aprendizaxe no ámbito tecnolóxico como un proceso permanente. Por iso, entre outras medidas, poñerase en marcha este ano, a Rede CeMIT de aulas de acceso público ás novas tecnoloxías que titorizará a cidadanía con maiores dificultades para poder integrar as TIC na súa vida cotiá. Ademais, a Rede promoverá a formación dixital entre os profesionais galegos e mostrará ás PEME e micropemes as vantaxes da sociedade da información. Dende estas aulas difundiranse os servizos de Administración electrónica e capacitarase aos cidadáns para empregalos.

e-Administración e Lexislación

Desde o punto de vista da secretaria xeral, a Lei 11/2007 encamíñase a implantar decididamente a Administración electrónica superando as disposicións de carácter simplemente facultativo contidas na Lei 30/1992, de Réxime Xurídico das Administracións Públicas e do Procedemento Administrativo Común.

Seguindo esta liña, recentemente, foi publicado no DOG o Decreto 198/2010 que establece o marco de desenvolvemento da Administración electrónica na Administración pública galega. Así, o obxectivo do Goberno galego é avanzar na mellora da calidade e da eficacia dos servizos ofrecidos e no impulso da eAdministración para unha maior eficiencia interna e nas relacións intra e interadministrativas. Trátase de conseguir unha Administración máis transparente e aberta aos cidadáns as 24 horas os 365 días do ano.

O cumprimento deste obxectivo supón para a Administración un gran reto, ao esixirlle dispoñer nun curto prazo (2013), de novos medios de comunicación e de ferramentas tecnolóxicas que se integren cos sistemas de información existentes e permitan a súa evolución futura, independentemente da súa implantación anterior paulatina.

Polo tanto, a Administración galega ofreceralles aos cidadáns a posibilidade de realizar as xestións de xeito telemático, con evidentes vantaxes para os usuarios: evítanse desprazamentos, os trámites pódense realizar en calquera momento e as xestións lévanse a cabo de xeito sinxelo. Ademais, supón un importante paso en materia de reutilización da información pública no noso país.

Así, a Xunta de Galicia por medio do protocolo de interoperabilidade que publicará este ano, establecerá os criterios e recomendacións que deberán ser tidos en conta para a toma de decisións tecnolóxicas que garantan a interoperabilidade e que eviten a discriminación aos cidadáns por razón da súa elección tecnolóxica. Ademais, debemos crear as condicións necesarias para asegurar un axeitado nivel de interoperabilidade que permita o exercicio de dereitos e o cumprimento de deberes a través do acceso electrónico aos servizos públicos.

"Queremos que co traballo de todos logremos unha Galicia 2.0", resume de xeito gráfico Mar Pereira.

O futuro

Desde o punto de vista da entrevistada, o principal reto de España e Europa nos próximos anos en canto á Administración Electrónica en termos xerais é tirar o máximo partido das TIC para evolucionar a Administración Pública a parámetros máis altos de intelixencia, sustentabilidade e innovación, e por conseguinte maximizar o seu potencial económico e social. "A certificación dixital e a sinatura electrónica son elementos moi importantes neste reto porque en moitos servizos en liña resulta esencial identificar e autenticar a persoa física ou xurídica á que se van prestar".

"A súa plena expansión deberá vencer as posibles barreiras que supoña a desconfianza por parte do cidadán", asegura Pereira. A falta de confianza no ámbito dixital e o incremento de formas de ciberdelincuencia, como o roubo de identidade, están a obstaculizar o desenvolvemento da economía en liña europea. As tecnoloxías de identificación electrónica (eID) e os servizos de autenticación son fundamentais para a seguridade das transaccións electrónicas, tanto no sector público coma no privado. Actualmente, o xeito máis corrente de autenticar é utilizar contrasinais, pero cada vez resulta máis necesario contar con solucións máis seguras que protexan a intimidade.

Outra barreira a resolver, en opinión da secretaria xeral, é a eliminación das fronteiras ou illas tecnolóxicas. "Debe facerse efectivo o concepto de interoperabilidade a todos os niveis e en particular no caso da acreditación dixital. Debe facerse efectivo o marco que formulan os Esquemas Nacionais de Seguridade e Interoperabilidade. Pero tamén Europa necesita unha mellor cooperación administrativa para desenvolver e implantar servizos públicos transfronteirizos en liña, incluídas unhas solucións prácticas de identificación e autenticación. É importante avanzar en iniciativas tales como o proxecto piloto a grande escala STORK, que permitan establecer unha plataforma europea de interoperabilidade da identificación electrónica coa finalidade de que os cidadáns accedan aos servizos de Administración electrónica dentro e fóra do seu país de orixe utilizando a súa identificación electrónica nacional".

2.10. Tractis

Tractis é unha plataforma web que permite negociar, xestionar e asinar contratos 100% en liña e con plena validez legal no mundo *offline*. Tractis permite a particulares e empresas facer negocios sen importar fronteiras, de forma eficiente e con absoluta seguridade e tranquilidade.

Negonation é o nome da empresa que está detrás de Tractis. A visión de Negonation é proporcionar xustiza transnacional en liña á nación Internet, creando as ferramentas que fagan posible un sistema de xustiza alternativo, máis eficiente e ao alcance de todos. Tractis é o primeiro paso. Trátase dun desafío enorme que implica estudo de lexislacións, integración con autoridades de certificación e tradución de idiomas a escala global.

2.10.1. Entrevista con David Blanco Giró

David Blanco Giró

CEO

Tractis

David Blanco: Non somos só tecnoloxía, dispoñemos dunha plataforma exclusivamente de servizos, unha característica diferencial respecto á competencia"

O cofundador de Tractis destaca que ofrecen soporte continuado a máis de 70 perfís de certificados de 28 Autoridades de Certificación en 12 países diferentes

Para Blanco os cidadáns valorarán o DNIe só cando poidan realizar con el os seus trámites habituais de xeito telemático e recoñecido tanto no ámbito público como privado

No ano 2006 xorde o proxecto Tractis, unha plataforma de comercio electrónico seguro orientada principalmente ao sector privado e co obxectivo claro de converterse no PayPal (sistema de pagamentos e transferencias monetarias a través da Internet) dos contratos. Con esta iniciativa, ponse por primeira vez a disposición das pequenas e medianas empresas unha tecnoloxía que, ata entón, resultaba prohibitiva para elas. Pero a visión da compañía vai máis aló. "Tractis non é só tecnoloxía, senón que ofrece unha plataforma de servizos de doado uso, pero única e exclusivamente de servizos, e esta é a nosa característica diferencial con respecto á competencia" destaca o cofundador da empresa, David Blanco. Con Tractis calquera persoa ou organización pode validar certificados, xa sexa con

propósito de autenticación ou de sinatura, e na actualidade a empresa ofrece un soporte continuado a 65 perfís de certificados de 12 países diferentes.

Segundo explica David Blanco, cando unha organización necesita ofrecer servizos como os de Tractis pode optar por un sistema de *outsourcing* ou ben de desenvolvemento interno. Polo xeral apóstase na integración con dúas ou tres autoridades de certificación, dado que a barreira de entrada para levar a cabo o desenvolvemento non é elevada, o que posibilita que se aborde internamente na empresa. O principal problema reside no mantemento dos devanditos servizos e, sobre todo, a apertura a calquera outro perfil de certificado español, europeo ou mundial. "É aí onde reside a vantaxe competitiva de ter a Tractis como socio tecnolóxico", apunta Blanco.

Usos do certificado dixital

Na actualidade o uso do certificado electrónico no ámbito privado obedece máis a unha necesidade competitiva entre as organizacións do sector que a unha necesidade real. Proba desta afirmación é o feito de que aínda non existan proxectos consolidados neste ámbito e, non obstante, si se desenvolveron iniciativas moi diversas en canto a certificados utilizados ou á limitación no uso de exploradores para utilizar os devanditos servizos. "Non" hai "unha necesidade aínda clara para pagar por esta tecnoloxía" detalla o responsable de Tractis, ao tempo que recorda que a actual situación de crise económica tamén supón un lastre á hora de impulsar e investir neste tipo de avances.

A pesar de que aínda se traballa para estender o uso e as vantaxes do certificado dixital, especialmente entre a cidadanía, hai que destacar o importante papel que España xogou e xoga a este nivel. España ocupa actualmente un posto moi relevante respecto ao resto de países en materia de implantación de certificación electrónica e, en concreto, do DNI electrónico. "Aínda que debemos avanzar no nivel de utilización do DNIe e das boas prácticas para manternos nese liderado, apunta David Blanco. Neste sentido aborda o distinto ritmo adoptado segundo cada país para o desenvolvemento do DNI electrónico.

Así, por exemplo, en Portugal ofrécese a posibilidade de comprar un lector electrónico no momento de renovar o documento de identidade; mentres que en Estonia, un país recoñecido na Unión Europea polo seu excelente nivel de boas prácticas, se inclúe o prezo do lector na renovación do DNI, polo que o usuario leva ao mesmo tempo un documento renovado e un lector para o seu uso, ofrecendo ademais a posibilidade de ser usado en múltiples servizos cotiáns, como os transportes públicos. Non obstante, España encóntrase no extremo oposto, xa que realiza campañas informativas entre os cidadáns unha vez emitido o DNIe, o que provoca unha efectividade moito menor entre a poboación que con outra xestión de tempos e programas. "Isto pode ser unha barreira ao uso do certificado electrónico e un freo á consolidación de España como líder en certificación electrónica", apunta o

cofundador de Tractis. Neste punto engade que "os cidadáns verán o valor do DNIe cando poidan realizar as súas transaccións habituais de xeito telemático e sexa recoñecido en calquera ámbito, tanto público coma privado.

En relación aos usos do DNI electrónico, David Blanco explica que un paso moi importante para o desenvolvemento desta iniciativa tecnolóxica foi a liberación dos comandos APDU do DNIe e, aproveitando este cambio, Tractis foi pioneira en darlles soporte aos comandos APDU do DNI electrónico. Isto permítelles aos clientes de Tractis utilizar o seu novo DNI electrónico sen necesidade de instalar previamente os *drivers* do DNIe, tarefa que, pola súa complexidade, deu dores de cabeza a ducias de miles de cidadáns.

Na actualidade pode considerarse que aínda se está na fase de despegue da implantación do uso do DNI electrónico. De feito, hoxe en día, aquelas organizacións que ofrecen servizos mediante este certificado dixital, como a banca, teñen aínda un volume de usuarios moi pequeno con respecto aos usuarios globais.

Neste punto, o impulsor de Tractis afirma que o papel que xoga a Fábrica Nacional de Moneda y Timbre (FNMT) nesta nova tecnoloxía non facilita a implantación de servizos de certificado electrónico. Unha das razóns é que, nestes momentos, o seu OCSP non é de libre consulta, o que incumpre un dos requisitos que se solicitan para dar sinatura electrónica recoñecida. Por outra banda, os cidadáns teñen a opción de utilizar o certificado da FNMT en lugar do DNIe e, como o seu uso é de momento máis sinxelo e cómodo, provoca a marxinación do DNI electrónico.

"Coa utilización do certificado electrónico existen moitas oportunidades de mellora nos procesos das organizacións que as fará ser máis competitivas e máis eficientes", sinala David Blanco. Neste sentido apunta o sector da banca, do que ofrece dous exemplos representativos como son a creación de contas aforro vivenda os últimos días do ano ou a formalización de préstamos hipotecarios. En ambos os dous casos o potencial cliente céntrase en dúas ou tres entidades ou produtos e se o primeiro que lle responde o fai conforme a mercado existen moitas posibilidades de formalizalo canto antes. "E nesa estratexia xoga un papel importante a axilidade para a sinatura e, polo tanto, poder realizalo cun certificado electrónico recoñecido, engade Blanco. Así, todo o proceso que agora tarda días e mesmo semanas se vería reducido a horas, "o que cambiaría as regras de xogo". "E Tractis céntrase nestes servizos", conclúe.

Retos de futuro

Os avances en materia de implantación e desenvolvemento de certificación dixital foron moitos nos últimos anos, especialmente en materia de fomento do uso do DNI electrónico, como a apertura de comandos APDU. A pesar disto, aínda se formulan outros moitos retos de futuro neste eido. Un dos

principais, a xuízo de David Blanco, é a necesidade de publicar un regulamento que desenvolva a lei de medidas de impulso á Sociedade da Información. Ademais, aposta por promover que os fabricantes de *hardware* inclúan nos seus produtos de serie lectores de DNI electrónico.

Por outra banda, sería conveniente incentivar o uso do DNIe fronte aos certificados electrónicos persoais que emite a FNMT, de xeito que a longo prazo soamente se tería un elemento de identificación para os cidadáns e para os trámites coas administracións públicas.

A nivel global, na actualidade estase a traballar en proxectos de integración como o *Stork*, co que se pretende alcanzar o recoñecemento panaeuropeo das identidades electrónicas e, en concreto, a aceptación do DNI electrónico e dos identificadores similares en servizos de Administración electrónica doutras administracións públicas europeas.

Plan estratéxico de Tractis

Un dos proxectos a curto prazo de Tractis é ofrecerlles ás administracións públicas os servizos da empresa de balde, o que lles facilitaría o cumprimento da lei sen ningún tipo de custo ou investimento engadido. Ademais, a visión global da entidade lévalles a establecer gran parte do seu mercado fóra das fronteiras españolas, en países como México ou Brasil, con millóns de persoas que "tarde ou cedo acabarán optando polo certificado electrónico e a utilización dos servizos de Tractis".

Consultado sobre as oportunidades de negocio que se abren a través do certificado dixital e os produtos e servizos asociados, o cofundador de Tractis teno claro: " Que non se faría sen certificado electrónico a longo prazo? Case nada", afirma, aínda que recoñece tamén que todo proceso de renovación tecnolóxica require o seu tempo de maduración, e nesta conxuntura encóntrase o certificado electrónico.

3.

SERVIZOS AO REDOR DA CERTIFICACIÓN DIXITAL

Neste apartado faise unha análise dos servizos e produtos ofrecidos actualmente polas organizacións, públicas e privadas máis representativas no sector da certificación dixital e a sinatura electrónica en España.

Aínda que se tiveron en conta para o estudo moitas organizacións, para a selección das entidades analizadas de xeito máis detallado seguíronse diversos criterios de relevancia como servizos ofrecidos, volume de certificados xestionados ou produtos máis innovadores. A información incluída neste apartado non pretende ser un catálogo comercial senón ofrecer unha visión ampla dos produtos e servizos xestionados polos diferentes prestadores de servizos en España.

Todas as organizacións seleccionadas para o estudo son prestadores de servizos de certificación segundo o establecido na Lei 59/2003, do 19 de decembro, de Firma Electrónica. Esta lei establece no seu artigo 30 e na disposición transitoria segunda que os prestadores de servizos de certificación deberán comunicarlle ao Ministerio de Industria, Turismo e Comercio os seus datos de identificación, os datos que permitan establecer comunicación co prestador, os datos de atención ao público, as características dos servizos que vaian prestar, as certificacións obtidas para os seus servizos e as certificacións dos dispositivos que utilicen.

Ademais, a lei indica que a información deberá ser convenientemente actualizada polos prestadores de servizos de certificación e será obxecto de publicación na dirección de Internet do citado Ministerio coa finalidade de outorgarlle a máxima difusión e coñecemento. A dirección de Internet de consulta é a seguinte:

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

Hai que ter en conta que de todos os certificados emitidos e servizos xestionados polos diferentes prestadores de servizos só se recollen polo MITyC na súa páxina de rexistro de prestadores aqueles relativos á sinatura electrónica, de persoa física e sistemas (as responsabilidades que lle asigna a Lei 59/2003 ao MITyC só abranguen o ámbito da sinatura electrónica), así como servizos relacionados como o de selado de tempo.

Toda a información analizada neste apartado procede, segundo o comentado, da páxina WEB do Ministerio de Industria, Turismo y Comercio, e amósase neste informe dun xeito mais accesible estructurándose en base a tipos específicos de certificados e servizos.

3.1. Servizos de certificación baseados en certificados recoñecidos

A relación de prestadores de servizos de certificación que realizaron a comunicación prevista no artigo 30.2 da Lei 59/2003 referente a **servizos de certificación baseados en certificados recoñecidos** son os seguintes:

Servizos de certificación baseados en certificados recoñecidos
AC AVOGACÍA
ANCERT - Axencia 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 Moeda (FNMT-RCM)
CICCP
Dirección Xeral da Policía e da Garda Civil - Corpo Nacional de Policía
EDICOM
Firmaprofesional, S.A.
Xerencia de Informática da Seguridade Social
HEALTHSIGN, S.L.
Izenpe, S.A
Ministerio de Defensa de España
REXISTRADORES DE ESPAÑA
Santander

A continuación faise unha relación dos certificados recoñecidos máis habituais xestionados polos diferentes prestadores de servizos de certificación:

CERTIFICADOS PARA PERSOAS FÍSICAS

É o certificado de acreditación de identidade. A entidade certificadora inclúe os datos persoais no certificado. Pode solicitarse por internet aínda que logo haberá que desprazarse ata unha oficina para acreditar a nosa identidade antes de que se xere o certificado.

Algúns exemplos deste tipo de certificados son os seguintes:

- **ACCV**: Certificados recoñecidos en soporte software para cidadáns e Certificados recoñecidos en dispositivo seguro para cidadáns (en tarxeta criptográfica)
- **CATCert**: idCAT, idCAT-CEX (cidadáns non residentes no Estado español) e CPISR-1
- **FNMT**: Certificado de Persoa Física
- **IZENPE**: Certificado de Cidadán (en tarxeta criptográfica) e Certificado de Asegurado do Sistema Sanitario de Euskadi (subscritor como asegurado do Sistema Sanitario de Euskadi)

CERTIFICADOS DE SINATURA MÓBIL

Os Certificados de Sinatura Móbil son certificados dixitais de persoa física emitidos para ser utilizados dende dispositivos móbiles.

Algúns exemplos deste tipo de certificados son os seguintes:

- **FIRMAPROFESIONAL**: Certificados de Sinatura Móbil
- **FNMT**: Certificado electrónico para asinar documentos e transaccións coa mesma validez legal que a sinatura manuscrita pero utilizando unha tarxeta SIM de telefonía celular

CERTIFICADOS DE REPRESENTANTE

Este tipo de certificados emítense para persoas físicas e determinan a relación de representación legal que ostenta a persoa titular con respecto á entidade ou persoa xurídica.

Un exemplo deste tipo de certificados é o seguinte:

- **CAMERFIRMA**: Certificado Cameral de Representante (representación xeral) e Certificado Cameral de Persona física de apoderamento especial (representación especial)

CERTIFICADOS DE PERTENZA Á ENTIDADE

Os certificados de pertenza á entidade identifican as persoas que desempeñan cargos ou postos en empresas ou entidades.

Neste certificado identifícase a empresa ou entidade de pertenza así como no seu caso o cargo ou posto desempeñado ou a relación de vinculación.

O subscritor adoita ser a persoa xurídica ou entidade identificada no certificado e os posuidores de claves as persoas físicas que posúen ou responden da custodia das claves de sinatura.

Algúns exemplos deste tipo de certificados son os seguintes:

- **CAMERFIRMA**: Certificado Cameral de Persoa Física de pertenza a Empresa/Entidade
- **CATCERT**: CPISR-1_C, CPISR-2_C (destinados a ser utilizados por cargos de organizacións alleas ás administracións públicas), CPISR-1_CE, CPISR-1_CU (para uso concreto), CPISR-2_E (estudante) e CPISR-2_EE (estudante estranxeiro)
- **FIRMAPROFESIONAL**: Certificado de Colexiado (profesionais colexiados en colexios profesionais) e certificado de Persoa Vinculada
- **IZENPE**: Certificado Corporativo Recoñecido (persoas que desempeñan cargos ou postos en entidades públicas que non exercen potestades administrativas) e Certificado Corporativo Privado Recoñecido (en tarxeta criptográfica)

CERTIFICADOS DE FACTURA ELECTRÓNICA

Os certificados de factura electrónica son certificados dixitais expedidos a persoas físicas vinculadas a unha determinada entidade, destinados a asinar facturas electrónicas en nome da devandita entidade. Este tipo de certificados son basicamente idénticos aos certificados de pertenza á empresa ou entidade salvo polo feito de que o subscritor do certificado está explicitamente autorizado para asinar facturas en nome da entidade á que está vinculado.

Algúns exemplos deste tipo de certificados son os seguintes:

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

CERTIFICADO ENTIDADE O DE PERSOA XURÍDICA

Certificados para persoas xurídicas emitidos a favor dunha entidade que actuará por medio dun representante legal ou voluntarios, responsable das claves, que poderá cedelas para o seu uso a unha terceira persoa ou aplicativo. Estes certificados permiten a un individuo actuar telematicamente en representación dunha persoa xurídica, de acordo co establecido no artigo 7 da Lei 59/2003, do 19 de decembro, de sinatura electrónica.

O grupo de usuarios que poden solicitar este tipo de certificados está composto polos administradores das entidades, os seus representantes legais e voluntarios con poder bastante para estes efectos.

A custodia dos datos de creación de sinatura asociados a cada certificado electrónico de persoa xurídica será responsabilidade da persoa física solicitante (sen prexuízo do cal poidan ser utilizados por outras persoas físicas vinculadas á entidade), cuxa identificación se incluirá no certificado electrónico.

Algúns exemplos deste tipo de certificados son os seguintes:

- **ACCV**: Certificado recoñecido de entidade (en tarxeta criptográfica)
- **CAMERFIRMA**: Certificado Cameral de Persoa Xurídica
- **CATCert**: CEISR-1 (en dispositivo seguro de creación de sinatura) e CEIXSA-1
- **FIRMAPROFESIONAL**: Certificado de Persoa Xurídica
- **IZENPE**: Certificado de Entidade

CERTIFICADO DE ENTIDADE SEN PERSONALIDADE XURÍDICA

Un exemplo deste tipo de certificados é o seguinte:

- **IZENPE**: Certificado de entidade sen personalidade xurídica (en tarxeta criptográfica)

CERTIFICADO DE ÓRGANO ADMINISTRATIVO

Este tipo de certificados identifican o órgano administrativo como asinante e á persoa física titular deste e deben ser solicitados por unha persoa no seu propio nome ou no dunha organización. En calquera caso, o subscritor é sempre o Órgano Administrativo identificado no certificado.

Estes certificados serán utilizados no ámbito das competencias propias do órgano administrativo e do posto ou cargo desempeñado.

Un exemplo deste tipo de certificados é o seguinte:

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

CERTIFICADOS ELECTRÓNICOS PARA A ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA DA ADMINISTRACIÓN PÚBLICA (SELO ELECTRÓNICO)

Este tipo de certificados teñen por obxecto garantir a identidade e a integridade para a actuación administrativa automatizada. Encóntranse enmarcados no ámbito da lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos público, e do real decreto 1671/2009, do 6 de novembro, polo que se desenvolve parcialmente esta.

Algúns exemplos deste tipo de certificados son os seguintes:

- **CAMERFIRMA**: Certificado de selo electrónico para actuación automatizada
- **CATCert**: CDA-1_SENM (selo electrónico de nivel medio de 1024 bits) e CDA-1_SENA (selo electrónico de nivel alto de 2048 bits)
- **FNMT**: Certificado electrónico para a actuación administrativa automatizada da Administración Pública, organismos e entidades públicas vinculadas ou dependentes
- **IZENPE**: Certificado para a actuación administrativa automatizada

CERTIFICADOS ELECTRÓNICOS PARA O PERSOAL AO SERVIZO DAS ADMINISTRACIÓNS PÚBLICAS

Este certificado ten por obxecto identificar e autenticar tanto o persoal ao servizo da Administración Pública como á Administración Pública mesma ou órgano no que presta os seus servizos. Encóntrase enmarcado no ámbito da lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos público, e o real decreto 1671/2009, do 6 de novembro, polo que se desenvolve parcialmente esta.

Algúns exemplos deste tipo de certificados son os seguintes:

- **ACCV**: Certificado recoñecido en dispositivo seguro para empregados públicos (en tarxeta criptográfica)
- **CAMERFIRMA**: Certificado de empregado público
- **FNMT**: Certificado electrónico para o persoal ao servizo das Administracións Públicas
- **IZENPE**: Certificado de Persoal das Entidades Públicas (en tarxeta criptográfica) e Certificado de Persoal do Goberno Vasco (en tarxeta criptográfica)

3.2. Servizos de certificación baseados en certificados non recoñecidos

A relación de prestadores de servizos de certificación que realizaron a comunicación prevista no artigo 30.2 da Lei 59/2003 referente a **servizos de certificación baseados en certificados non recoñecidos**:

Servizos de certificación baseados en certificados non recoñecidos
CAMERFIRMA
CATCert
CERES Fábrica Nacional de Moeda e Timbre - Real Casa da Moeda (FNMT-RCM)
Colexio Oficial de Arquitectos de Sevilla
ipsCA
Izenpe, S.A
Ministerio de Defensa de España
Servizo de Saúde de Castela-A Mancha (SESCAM)
Telefónica Empresas

A continuación faise unha relación dos certificados non recoñecidos máis habituais xestionados polos diferentes prestadores de servizos de certificación:

CERTIFICADO DE DISPOSITIVO APLICACIÓN

Este tipo de certificados utilízanse para, almacenados nun servidor (é un certificado de compoñente que está asociado normalmente a unha clave custodiada por unha máquina) e requiridos por unha aplicación, asinar documentos ou mensaxes. Estes certificados emítense a persoas xurídicas responsables da operación de aplicacións informáticas que se identifican dixitalmente, asinan electronicamente *webservices* ou outros protocolos e que reciben documentos e mensaxes cifradas.

Son certificados ordinarios, e que garanten a identidade da persoa responsable e a integridade e a autenticidade dos datos asinados. Tamén permiten a recepción de información cifrada.

Algúns exemplos deste tipo de certificados son os seguintes:

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

CERTIFICADO DE PERSOA XURÍDICA E ENTIDADES SEN PERSONALIDADE XURÍDICA

Un exemplo deste tipo de certificados é o seguinte:

- **FNMT**: Certificados non recoñecidos de persoa xurídica e entidades sen personalidade xurídica (para o ámbito tributario)

CERTIFICADOS DE PERTENZA Á EMPRESA

O subscritor será a persoa xurídica identificada no certificado e os posuidores das claves as persoas físicas que posúen ou responden da custodia das claves de sinatura.

Un exemplo deste tipo de certificados é o seguinte:

- **IZENPE**: Certificado privado non recoñecido (en tarxeta criptográfica)

CERTIFICADOS DE PERTENZA Á ENTIDADE PÚBLICA

É o certificado no que se identifica persoas que desempeñan cargos ou postos en entidades públicas que non exercen potestades administrativas. Trátase dun certificado no que o subscritor será necesariamente a mesma entidade usuaria. Neste certificado inclúese a entidade pública de pertenza así como, se é o caso, o cargo desempeñado.

Un exemplo deste tipo de certificados é o seguinte:

- **IZENPE**: Certificado corporativo non recoñecido

3.3. Servizos en relación coa sinatura electrónica

A relación de prestadores de servizos de certificación que realizaron a comunicación prevista no artigo 30.2 da Lei 59/2003 referente a **outros servizos en relación coa sinatura electrónica**:

Outros servizos en relación coa sinatura electrónica - Servizos de validación temporal
ANF AC
Autoritat de Certificació de la Comunitat Valenciana - ACCV
CAMERFIRMA
CERES Fábrica Nacional de Moeda e Timbre - Real Casa da Moeda (FNMT-RCM)
EADTrust
EDICOM
Firmaprofesional, S.A.
Xerencia de Informática da Seguridade Social
Izenpe, S.A
Ministerio de Defensa de España
Tractis

Outros servizos en relación coa sinatura electrónica - Servizos de validación de certificados
CertiVer
EADTrust
Tractis

Outros servizos en relación coa sinatura electrónica - Servizos de custodia
CERES Fábrica Nacional de Moeda e Timbre - Real Casa da Moeda (FNMT-RCM)
Tractis

Outros servizos en relación coa sinatura electrónica - Outros servizos
CERES Fábrica Nacional de Moeda e Timbre - Real Casa da Moeda (FNMT-RCM)
EDICOM
Firmaprofesional, S.A.
Izenpe, S.A

A continuación faise unha relación dos servizos máis habituais xestionados polos diferentes prestadores de servizos de certificación neste ámbito:

SERVIZO DE SELADO ELECTRÓNICO

O selado electrónico de documentos ou *timestamping* é o complemento ideal da sinatura electrónica xa que é un sistema polo que un terceiro asegura que os datos contidos nun documento existen dende unha data concreta.

A sinatura electrónica adoece deste defecto, e é que non temos a certeza de cando se asinou o documento electrónico. Para certo tipo de contratos a data non é un dato esencial, pero para outros como pode ser a contratación dun seguro, convértese en algo tan importante como a mesma sinatura. O mesmo podemos establecer para un contrato de servizo ou para selar unha reclamación, como pode ser ante a administración.

Trátase, polo tanto, da emisión de selos de tempo que permitan asociar unha actuación cunha data e hora, e así obter evidencias técnicas e xurídicas de que tal acto se produciu nun determinado momento de tempo.

Algúns exemplos deste tipo de servizo son os seguintes:

- **ACCV**: Servizo de selado de tempo (xeración e emisión de selos de tempo para organismos da Generalitat Valenciana, así como para calquera outra administración ou entidade pública coa que se asinase o correspondente convenio de certificación)
- **CAMERFIRMA**: Selado de tempo
- **EADTrust**: Servizo de selado de tempo
- **FIRMAPROFESIONAL**: Servizo de selado de tempo
- **FNMT**: Servizo de *timestamping*
- **IZENPE**: Servizo de selado de tempo

- **TRACTIS**: Servizo de selado de tempo

SERVIZO DE CONSTANCIA E ACREDITACIÓN DA PUBLICACIÓN

Este servizo serve para actuar como Terceiro de Confianza de modo que dea fe da publicación a partir dun determinado momento no tempo e que ata outra data determinada a devandita publicación non foi modificado nin permaneceu accesible. Deste modo, calquera entidade, pública ou privada, poderá contar un terceiro que demostre fidedignamente que un documento foi publicado e permaneceu inalterado e accesible no tempo.

Un exemplo deste tipo de servizo é o seguinte:

- **IZENPE**: Servizo de Constancia e Acreditación de Publicación

SERVIZO DE CUSTODIA DE DOCUMENTOS ELECTRÓNICOS

A custodia das transaccións e documentos electrónicos é un factor importante no desenvolvemento das relacións electrónicas entre partes xa que permite dotar estas de seguridade xurídica preventiva preconstituíndo tanto unha proba testemuñal como documental da realización da transacción entre as partes. O servizo de custodia de documentos electrónicos é un servizo, cuxo acceso se realiza mediante identificación por procedementos de sinatura electrónica. O servizo prové aos clientes dun sistema de depósito de documentos electrónicos realizado por un terceiro capaz de dar fe da existencia e contido do documento.

Un exemplo deste tipo de servizo é o seguinte:

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

SERVIZO DE VALIDACIÓN DE CERTIFICADOS

Trátase de servizos que proporcionan información acerca do estado de validez de diferentes tipos de certificados emitidos por un ou varios Prestadores de Servizos de Certificación (servizos semellantes aos que **@firma** presta no sector público).

Algúns exemplos deste tipo de servizo son os seguintes:

- **EADTrust**: Servizo de validación de certificados
- **Tractis**: Servizo de autoridade de validación semántica

3.4. Outros Servizos

Como se comentou anteriormente, hai que ter en conta que de todos os certificados e produtos ofrecidos polos diferentes prestadores de servizos de certificación só se recollen polo MITyC, na súa páxina de rexistro de prestadores, aqueles relativos á sinatura electrónica, de persoa física e sistemas, así como servizos relacionados como o de selado de tempo. Estes certificados e servizos foron os analizados nos apartados 3.1, 3.2 e 3.3 deste informe.

Neste apartado analízanse outros servizos ofrecidos polos prestadores de servizos á marxe dos relacionados estritamente coa sinatura electrónica e o selado de tempo.

3.4.1. Certificados

CERTIFICADO DE SEDE

Os certificados recoñecidos de Sede Electrónica serven para identificar un portal WEB e establecer comunicacións seguras, de tal forma que se garante a privacidade e integridade da información que se ofrece, excluíndo a posibilidade de ser vítimas dunha fraude.

A Lei 11/2007 de Acceso Electrónico dos Cidadáns aos Servizos Públicos define a Sede Electrónica como a dirección electrónica dispoñible para os cidadáns a través de redes de telecomunicacións cuxa titularidade, xestión e administración corresponde a unha Administración Pública, órgano ou entidade administrativa no exercicio das súas competencias.

As Sedes Electrónicas deben dotarse de ferramentas criptográficas:

Identificar o sitio web e a súa vinculación cunha determinada Administración Pública.

Garantir a privacidade das comunicacións, é dicir, que a información intercambiada entre un cidadán usuario desa Sede e a propia Sede sexa cifrada.

A autenticación ou identificación das sedes electrónicas realizarase mediante a utilización de certificados dixitais de sede electrónica (Artigo 18 Real Decreto 1671/2009).

O certificado recoñecido de Sede Electrónica basicamente é un certificado de servidor WEB seguro que inclúe a identificación do titular da Sede Electrónica, e que se emite nun dispositivo seguro ou medio equivalente.

Algúns exemplos deste tipo de certificado son os seguintes:

- **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 e Sede Electrónica con EV (validación estendida que achega melloras de protección ao usuario)

CERTIFICADOS DE CLIENTE SEGURO

Son certificados empregados para identificar e autenticar clientes ante servidores en comunicacións mediante o protocolo *Secure Socket Layer*, e expídense normalmente a unha persoa física, ben un particular, ben un empregado dunha empresa.

CERTIFICADOS DE SERVIDOR SEGURO

Son certificados empregados para identificar un servidor ante un cliente en comunicacións mediante o protocolo *Secure Socket Layer*, e expídense xeralmente a nome da empresa propietaria do servidor seguro ou do servizo que este vai ofrecer, vinculando tamén o dominio polo que se debe acceder ao servidor. A presenza deste certificado é condición imprescindible para establecer comunicacións seguras SSL.

CERTIFICADOS DE SINATURA DE CÓDIGO

Os certificados de sinatura de código son unha ferramenta cada vez máis utilizada polos desenvolvedores para a sinatura electrónica de aplicativos.

A sinatura electrónica de código permite distribuír de forma segura ActiveX, Macros, Applets, MIDlet (J2ME) garantindo a autenticidade e integridade do contido antes de ser executado, e desta forma eliminando riscos.

3.4.2. Produtos e solucións

Neste apartado analízanse algúns produtos e solucións ao redor da sinatura electrónica de especial interese:

3.4.2.1. Servizos de validación de certificados dixitais

Este tipo de servizos permiten a consulta do estado dos certificados. O validador responde se un certificado é válido ou non é válido (por exemplo, porque está revogado) e na mesma resposta tamén devolve información adicional, como por exemplo, datos útiles do certificado dixital (por exemplo o nome e apelidos, o DNI, etc.) e o nivel de seguridade asociado ao certificado dixital.

Xeralmente este tipo de servizos recoñecen múltiples prestadores de servizos de certificación, uniformando a información asociada aos certificados, soportan os mecanismos de validación de certificados estándares e admite a integración de calquera outro mecanismo personalizado.

Lístas de certificados revogados (CRL**)** conteñen o número de serie de todos os certificados emitidos por unha Autoridade de Certificación e que, por algún motivo deixaron de ser válidos de xeito previo á expiración do seu período de validez orixinal. Para saber se un certificado é de confianza debe comprobar se o número de serie deste está incluído na CRL publicada pola Autoridade de Certificación emisora. Se é así, o certificado foi revogado e non é de confianza.

Os **servizos** OCSP (*Online Certificate Status Protocol*), definidos no estándar RFC-2560, proporcionan aos usuarios e as aplicacións un método áxil e rápido de obter o estado dun certificado, evitando ter que descargar a Lista de Certificados Revogados (CRL).

3.4.2.2. Servizos de validación de sinaturas dixitais

Este tipo de servizos permiten realizar comprobacións sobre a validez dunha sinatura dixital. O servizo inspecciona a sinatura e verifica, por unha parte, que a sinatura estea ben formada e, por outra parte, comproba o estado do certificado no momento que se produciu a sinatura. En función dos resultados anteriores responde se a sinatura é válida ou non é válida.

3.4.2.3. Sinatura electrónica en aplicacións

Xeralmente son compoñentes software (*applets* ou similares) que facilitan a integración da funcionalidade de sinatura electrónica en aplicacións web, e que permiten asinar diferentes formatos de documentos e con diferentes formatos de sinatura.

3.4.2.4. Preservación e arquivo electrónico de documentos

Trátase de servizos que garanten que os documentos que xera ou recibe unha organización no exercicio das súas funcións se manteñen íntegros, fiables, auténticos e accesibles ao longo do seu ciclo de vida.

Este tipo de servizos inclúe xeralmente:

- A creación dunha plataforma tecnolóxica de arquivo dixital ou repositorio para almacenar os documentos electrónicos que poida garantir ao longo do tempo a autenticidade, a fiabilidade, a integridade, a seguridade e a dispoñibilidade dos documentos electrónicos e a súa información.
- desenvolvemento de estratexias ou solucións tecnolóxicas para tratar os problemas derivados da durabilidade dos soportes e a obsolescencia da tecnoloxía.
- A implantación dun sistema de xestión da información é clave para optimizar os procesos e mellorar o servizo ofrecido e a seguridade da información.
- A custodia de documentos é un paso máis na xestión documental e implica a existencia dun terceiro que se responsabiliza de arquivar, con garantías técnicas e legais, os documentos doutras organizacións.

Existen diversas entidades e empresas que ofrecen o servizo de custodia de información baseado no almacenamento de documentos, tanto asinados dixitalmente e/ou cifrados como sen asinar e/ou cifrar e garantindo que o documento custodiado mantén ao longo do tempo o mesmo valor legal.

Para manter a validez legal no tempo defínese, en función dos diferentes prazos de custodia (curto, medio e longo prazo), a tecnoloxía e os soportes a utilizar así como os formatos aceptados e o seu mantemento. Ademais, xeralmente, incorpórase un selado de tempo nos documentos asinados que asegura o momento de realización da sinatura e a validez do certificado co que se realizou esta.

3.4.2.5. Broker de identidades

Os broker de identidades son "axentes mediadores" que se ocupan de facilitar información asociada coa identificación dun cidadán que non obre en poder daquel que xestiona o servizo.

Nunha sociedade con cidadáns desenvolvendo trámites ou actividades en diversos municipios ou entidades fronte ás posibles necesidades informativas é precisa a comunicación entre elas, así como que se establezan convenios de colaboración entre elas. Os *brokers de*

identidades xorden para realizar os labores de intermediación entre as entidades de modo que para aquelas que queiran chamar servizos a través desta plataforma as chamadas sexan sempre co mesmo formato independentemente do provedor do servizo. Ademais permiten a solicitude dun servizo a varias entidades á vez ou a relación con outros axentes de intercambio.

3.4.2.6. Facturación electrónica

A facturación electrónica é un equivalente funcional da factura en papel e consiste na transmisión das facturas ou documentos análogos entre emisor e receptor por medios electrónicos (ficheiros informáticos) e telemáticos (dun ordenador a outro), asinados dixitalmente con certificados recoñecidos. Dependendo do volume das empresas, o aforro por concepto de administración de facturas (recepción, almacenaxe, busca, sinatura, devolución, pagamento, envío, etc.) pode flutuar entre o 40% e o 80%.

Nun sistema de facturación electrónica, por cada factura intercambiada débese achegar a sinatura electrónica desta, xerada cos datos de sinatura do emisor, e todos os datos que permitan ao receptor verificar a integridade do asinado e a autenticidade do asinante. Os algoritmos criptográficos utilizados tanto para o *hash* do documento como para a sinatura electrónica deben estar plenamente aceptados pola comunidade internacional (SHA1, MD5, RSA etc.).

O receptor da factura electrónica deberá dispoñer do software que permita verificar a sinatura da factura e a identidade do emisor, así como que o certificado utilizado para a xeración da sinatura electrónica é válido (non está revogado nin caducado).

Existen no mercado diferentes solucións para aquelas empresas e traballadores autónomos que desexen realizar a facturación electrónica dunha forma doada. Estas solucións, que serven para realizar tarefas tales como crear, asinar ou enviar facturas, están orientadas a usuarios que non dispoñen de coñecementos avanzados para esta tarefa.

A facturación electrónica require de certificados de sinatura dixital necesarios para poder emitir unha factura para que esta teña validez. Os certificados dixitais válidos para a emisión de facturas electrónicas deben:

Seguir o estándar UIT X.509 versión 3 ou superior

Estar emitidos por unha Autoridade de Certificación admitida nas relacións tributarias por medios electrónicos e telemáticos coa Axencia Estatal de Administración Tributaria (AEAT).

4.

ANÁLISE DA LEXISLACIÓN ACTUAL

Neste apartado desenvólvese unha ampla análise da lexislación actualmente vixente en materia de identidade e sinatura electrónica.

Para o elaboración deste apartado contase coa colaboración do avogado Víctor Salgado Seguín do bufete Pintos & Salgado Avogados. O bufete Pintos & Salgado Avogados, especializado na aportación de solucións xurídicas no eido das novas tecnoloxías, conta con máis de dez anos de experiencia en consultoría legal informática, propiedade intelectual e auditoría e implantación da normativa de proteción de datos de carácter persoal.

4.1. Marco Xeral

Non nos queda máis remedio que admitir que estamos demasiado apegados á tinta e ao papel. Crecemos con estes medios e, polo tanto, atribuímoslle a máxima credibilidade. Historicamente, todo o que podemos tocar e, mesmo ulir, nos achega moita máis seguridade sobre a fiabilidade e realidade das cousas.

É verdade que en moitas ocasións é conveniente, e mesmo necesario, que exista unha proba documental escrita para os efectos de verificar a existencia dunha relación xurídica ou dun feito determinado, xa sexa pola súa importancia intrínseca ou xa por esixencia legal. Non obstante, debemos decatarnos que no mundo dixital que nos rodea, e grazas á nosa nova lexislación que teremos oportunidade de comentar, que algo conste "por escrito" non será nunca máis sinónimo de necesariamente "en papel". Máis ben todo o contrario.

Unha das primeiras normas que o fixeron posible foi o, xa derrogado, Real Decreto-Lei 14/1999, do 17 de setembro, polo que se regulou por vez primeira a sinatura electrónica no noso país. Con esta regulación, España converteuse nun dos primeiros países, a nivel mundial, en recoñecer legalmente a validez dun documento electrónico asinado dixitalmente.

A sinatura electrónica, como veremos, é un medio de proba mesmo máis seguro e fiable cá familiar sinatura manuscrita. Isto é debido a que, grazas á maxia da súa tecnoloxía, a mesma non só nos indica "quen asina" senón tamén o que asina xa que, como gran novidade, se vincula ao propio texto do documento a asinar (o cal en papel é imposible).

Non obstante, a pesar deste temperán recoñecemento xurídico e das súas grandes vantaxes para a seguridade probatoria, o certo é que o seu uso na práctica foi marxinal.

A pesar diso, algúns servizos e trámites como a declaración de impostos a través de Internet foron unha honrosa excepción e un bo exemplo dunha ampla implantación e indubidable utilidade da sinatura electrónica no noso país. Co fin de que este exemplo poida xeneralizarse, o Parlamento aprobou unha serie de normas destinadas, non só a ampliar o seu recoñecemento, senón especialmente a fomentar o seu uso. Destacamos especialmente tres:

En primeiro lugar, a Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico, pola que se recoñece por vez primeira a equivalencia xurídica da palabra "escrito" á palabra "electrónico", falando de contratos e sempre que se garanta a súa proba mediante soporte dixital.

En segundo lugar, a Lei 59/2003, do 19 de decembro, de Firma Electrónica, que substituíu

a citada norma do 99, contemplou, entre outras novidades, a creación do DNI dixital, coa conseguinte xeneralización da tenza (que non do uso) da sinatura electrónica no noso país.

E, en terceiro lugar, Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos, que garante o dereito de todos a relacionarnos coas Administracións Públicas a través de medios electrónicos e, principalmente, a través do uso da sinatura electrónica legalmente recoñecida.

A continuación, daremos un rápido repaso aos aspectos fundamentais desta normativa:

4.2. Cara á identidade dixital

Como comentamos, dende 1999 España foi pioneira en lexislar sobre a sinatura electrónica. Actualmente, esta xa se recoñece na práctica totalidade de países desenvolvidos e, no noso país, regúlase agora mediante a Lei 59/2003, do 19 de decembro, de Firma Electrónica.

A pesar diso, é aínda unha gran descoñecida para a gran maioría dos cidadáns. Por exemplo, se preguntásemos a un grupo amplo de persoas cantos teñen sinatura electrónica, seguramente moi poucos responderían afirmativamente. Hai pouco, fixemos este pequeno experimento con alumnos na universidade e, a esta pregunta, menos dun 5% levantaron a man positivamente.

Por outro lado, se preguntamos cantos renovaron recentemente o seu DNI, sen dúbida contestarán moitos máis afirmativamente. Cando repetimos esta mesma pregunta na universidade, levantaron a man case un 50% dos asistentes.

Pois, repito o mesmo que lles dixemos no seu día aos nosos alumnos: "os segundos deberiades ter levantado a man ao principio. Saibádelo ou non, o voso recente DNI (ese que ten un pequeno *chip* como a tarxeta do Bus) incorpora xa a vosa sinatura electrónica neste. Polo tanto, ¡xa tedes sinatura electrónica! ".

Polo tanto, só temos que ser conscientes diso.

¿Onde poderemos usala?

Pois nun gran número de transaccións en Internet. Co tempo serán practicamente as mesmas que no mundo físico.

Isto é debido, entre outras normas, tamén ao artigo 23 da Lei 34/2002, do 11 de xullo, de Servizos da Sociedade da Información e de Comercio Electrónico (LSSICE), sobre a base do cal serán válidos todos os contratos que realicemos a través da Rede, mesmo os que a Lei esixa "por escrito":

"1. Os contratos celebrados por vía electrónica producirán todos os efectos previstos polo ordenamento xurídico,(...).

3. Sempre que a Lei esixa que o contrato ou calquera información relacionada con este conste por escrito, este requisito entenderase satisfeito se o contrato ou a información se contén nun soporte electrónico. "

De feito, os únicos ámbitos que quedan exceptuados do anterior son os seguintes:

Os contratos relativos ao Dereito de familia e sucesións.

Os documentos e escrituras públicas.

Por suposto, o DNIe non é a única sinatura electrónica válida no noso país. Hai moitas outras recoñecidas que son emitidas por empresas e entidades de todo tipo para o seu uso en distintos ámbitos cumprindo os requisitos estipulados na Lei.

A continuación veremos os aspectos básicos da devandita normativa:

4.3. A sinatura electrónica (Lei 59/2003)

Concepto e Tipos de Sinatura Electrónica

De acordo, falamos das súas vantaxes e virtudes xurídicas pero, ¿que é a sinatura electrónica?

O artigo 3.1 da Lei 59/2003 de Firma Electrónica, defínea como "o conxunto de datos en forma electrónica, consignados xunto a outros ou asociados con eles, que poden ser utilizados como medio de identificación do asinante,".

Sen dúbida, é unha definición bastante ambigua pero que xa nos define os tres elementos principais da sinatura electrónica:

É un "conxunto de datos" en formato dixital, podendo compoñerse de texto, números ou outros símbolos;

Que están situados xunto a outros, que supoñerían o "texto ou datos asinados", podendo mesmo estar asociados con eles (xa sexa mediante fórmulas matemáticas ou doutro modo) e

Que poden identificar o asinante: este, sen dúbida, é o elemento clave e todo o texto da Lei se encamiña a reforzar esta identificación de modo único e válido xuridicamente.

Pero, ¿todas as sinaturas electrónicas son iguais?

Obviamente, non. Dependerá de diversos factores que influirán no seu maior ou menor recoñecemento e validez probatoria.

Deste modo, o artigo 3 da lei fálanos tamén dos diversos tipos de sinatura electrónica. Define, fundamentalmente catro tipos:

A sinatura electrónica avanzada;

A sinatura electrónica recoñecida;

A sinatura electrónica non recoñecida e

finalmente, a que denominaremos como sinatura electrónica acordada.

Imos ver rapidamente cada unha destes catro tipos de sinatura electrónica:

A sinatura electrónica avanzada

A sinatura electrónica avanzada defínese como aquela que cumpre os seguintes requisitos:

Permite identificar o asinante e detectar calquera cambio ulterior dos datos asinados;

Está vinculada ao asinante de xeito único e aos datos a que se refire; e

Foi creada por medios que o asinante mantén baixo o seu exclusivo control.

Aínda que a lei, obviamente, non pode decantarse por un ou outro tipo de tecnoloxía concreta debido ao principio de neutralidade tecnolóxica, é evidente que a sinatura electrónica avanzada se refire á tecnoloxía amplamente utilizada e difundida na actualidade de "criptografía de clave asimétrica".

Isto dedúcese dos elementos identificativos que acabamos de resumir. O primeiro deles, refírese a que non só debe permitir identificar o asinante senón que ademais a devandita sinatura debe detectar calquera cambio posterior nos datos asinados. Esta é unha característica fundamental da criptografía de clave asimétrica, que se define como "integridade" da sinatura e que é debida a que esta vai vinculada ao texto sobre o cal se está a aplicar. Iso significa que calquera alteración posterior do texto ou datos asinados en primeira instancia, aínda que fose de "unha soa coma", supoñerá un erro, xa non da sinatura en si mesma, senón da súa aplicación sobre os datos asinados.

Poñereivos un exemplo práctico:

Se eu vos pedise que me asinásedes un autógrafo nun papel en branco (por se un día sodes famosos), sen dúbida moitos non teriades reparos en facelo.

Agora ben, se eu vos dixese que nos devanditos papeis posteriormente imprimirei o seguinte: "Eu, fulano de tal, pola presente declaro que lle debo 5.000 euros a fulano en concepto de préstamo persoal o cal será devolto á súa solicitude" Como probariades que o devandito documento é falso?

O certo é que o teriades moi difícil posto que a proba máis estendida para iso é a pericial caligráfica sobre a vosa sinatura, e a devandita proba diría que efectivamente esta é vosa.

É dicir, en papel non hai modo de saber que estaba escrito no momento da sinatura (polo menos de xeito sinxelo).

Porén, isto non acontece coa sinatura electrónica avanzada. De feito, esta xérase a partir do texto que estamos a asinar. Deste modo, se alguén cambiase ou engadise unha soa coma ao documento electrónico asinado, a devandita sinatura sería inválida: unha proba sinxela diríanos que si é a nosa sinatura pero que non é o texto que asinamos orixinalmente.

Isto é o que chamamos "integridade" da sinatura electrónica e en Dereito é como descubrir a pedra filosofal que pode rematar con todas as falsidades documentais e aumenta, polo tanto, a seguridade xurídica dos documentos electrónicos por enriba dos seus homólogos en papel.

A sinatura electrónica recoñecida

Esta sinatura é a única sinatura electrónica cuxo valor xurídico e probatorio se equipara plenamente á sinatura manuscrita na lei.

En realidade, é unha sinatura electrónica avanzada que ademais cumpre as características seguintes:

Estar baseada nun "certificado recoñecido" e

Estar xerada por un "dispositivo seguro de creación de sinatura".

Estes dous elementos adicionais confiren a esta sinatura unha seguridade xurídica completa.

Pero, que é un certificado?:

O artigo 6.1 da Lei de Firma Electrónica define o certificado electrónico como "un documento asinado electronicamente por un prestador de servizos de certificación que vincula uns datos de verificación de sinatura a un asinante e confirma a súa identidade".

Este documento ten unha importancia vital posto que relaciona de xeito inequívoco a unha clave pública concreta co seu posuidor legal e confirma plenamente a súa identidade. Sen esta confirmación documental, non teriamos xeito de saber se a persoa que aparece como titular da clave é, en realidade, a súa propietaria.

O devandito documento deberá ir asinado, á súa vez, por un "terceiro de confianza" ou, como o denomina a lei, un prestador de servizos de certificación. Este prestador deberá establecer algún mecanismo para verificar a devandita identidade ademais de someterse a un réxime de responsabilidade concreto sobre a devandita identificación.

Isto en canto a un certificado electrónico, pero que é un "certificado recoñecido"?

O artigo 11.1 da Lei define o certificado recoñecido como aquel certificado electrónico expedido por un prestador de servizos de certificación que cumpra un requisitos especiais, precisamente, en canto á comprobación da identidade e demais circunstancias dos solicitantes e, por outro lado, á fiabilidade e as garantías dos seus servizos.

Entre outros requisitos, o artigo 20.2 da Lei establece a obriga de contar cun seguro de responsabilidade civil de 3 millóns de euros para responder pola súa actividade.

A sinatura electrónica non recoñecida

Este tipo de sinatura é especialmente importante no que se refire á validez xurídica última doutros tipos posibles de sinatura electrónica distintos aos que acabamos de analizar.

Así, o artigo 3.9 da Lei de Firma Electrónica, determina que "non se lle negarán efectos xurídicos a unha sinatura electrónica que non reúna os requisitos de sinatura electrónica recoñecida en relación aos datos aos que estea asociada polo simple feito de presentarse en forma electrónica".

Isto supón, ao cabo, un recoñecemento implícito da validez xurídica doutros tipos de sinatura electrónica, sempre e cando esteamos en disposición de probar a súa correcta emisión, vinculación, configuración e solidez técnica e xurídica.

Todo iso deberá ser acreditado, no seu momento, polo titular, asinante ou parte interesada dentro dun procedemento legal.

A sinatura electrónica acordada

O apartado 10 do artigo 3 da Lei de Firma Electrónica incorpora un último tipo de sinatura que nós denominamos como "asinatura electrónica acordada".

Este apartado dispón que: "para os efectos do disposto neste artigo, cando unha sinatura electrónica se utilice conforme ás condicións acordadas polas partes para relacionarse entre si, terase en conta o estipulado entre elas".

Isto significa que, calquera que fose o sistema de sinatura electrónica que se utilizase, se o devandito sistema fose convido ou acordado polas partes dun contrato, este tería plena validez xurídica e probatoria entre estas, sempre e cando se cumpran os requisitos estipulados no devandito contrato.

Isto abre a vía para que sistemas menos formais ou convencionais poidan ter pleno valor probatorio en ámbitos pechados ou cun número limitado de intervenientes.

O DNI dixital

Como adiantabamos anteriormente, o artigo 15 da Lei de Firma Electrónica, define o Documento Nacional de Identidade Electrónico como aquel documento que:

Por un lado, acredita electronicamente a identidade persoal do seu titular e,

Por outro lado, permite así mesmo a sinatura electrónica de documentos.

A grande importancia que ten a emisión deste novo documento nacional de identidade

é que o propio artigo 15 ditamina que "todas as persoas físicas ou xurídicas, públicas ou privadas deberán recoñecer a súa eficacia".

Polo tanto, o documento nacional de identidade electrónico é a única sinatura electrónica recoñecida que o é simplemente polo seu simple recoñecemento expreso na propia lei.

Para usala, non obstante, necesítase un lector especial do *chip* que leva o propio DNI. Os ordenadores deberían traelos de serie en breve pero, mentres tanto, pódense comprar en tendas especializadas por un prezo alcanzable, acolléndonos a ofertas periódicas dos provedores con prezos reducidos ou, mesmo, de modo gratuíto como medidas de impulso do uso do e DNI subvencionadas polo Goberno.

Hoxe en día, cada vez son máis os servizos de Internet onde podemos utilizar o DNIe: principalmente no ámbito das administracións públicas (Facenda, Seguridade Social, Concellos, etc.) pero tamén comeza a introducirse no ámbito privado, onde podemos ver xa algúns bancos e caixas de aforro que o utilizan como forma alternativa aos seus tradicionais (e, en ocasións, menos seguras) claves de acceso.

Validez probatoria, aplicación e usos

Como vimos, hoxe en día xa se admite a plena validez xurídica da sinatura electrónica a un mesmo nivel mesmo que a sinatura manuscrita, pero que documentos se poden asinar dixitalmente?

O certo é que, grazas á nosa avanzada lexislación, son xa practicamente todos:

Todo tipo de contratos, mesmo os que se esixan en "forma escrita", a excepción dos de familia, sucesións e escrituras públicas. (como vimos, grazas ao artigo 23 da LSSICE).

As facturas, sempre que se cumpran os requisitos establecidos na Lei 56/2007, do 28 de decembro, de Medidas de Impulso á Sociedade da Información (LMISI) e normativa concordante.

Declaracións e documentos para as Administracións Públicas, posible dende hai anos no ámbito fiscal ou laboral pero cun impulso importante a partir da Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos (LAECSP).

E, en definitiva, todos aqueles outros documentos respecto dos cales non se regulasen requisitos formais para a súa validez.

E, no seu caso, ¿como se pode presentar unha sinatura electrónica como proba nun procedemento?

O artigo 3. 8 da Lei de Firma Electrónica dispón que "o soporte en que se achen os datos asinados electronicamente será admisible como proba documental en xuízo".

Isto significa que calquera persoa ou parte interesada nun procedemento xudicial poderá achegar calquera documento directamente en formato dixital ou electrónico como proba documental en xuízo sen que se lle poida esixir a súa transposición a calquera outro soporte non dixital. Por exemplo, impresión en papel ou outro sistema análogo.

4.4. As Administracións Públicas fronte ao cidadán dixital (Lei 11/2007)

A Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos Servizos Públicos dispón que todas as Administracións Públicas deberán estar plenamente accesibles na Rede para os cidadáns.

Sobre a base del, calquera procedemento, servizo ou trámite prestado por un Concello, unha Comunidade Autónoma ou un Ministerio deberá estar tamén dispoñible por medios electrónicos.

Así, o artigo 6.1 da citada Lei 11/2007, tamén denominada como Lei de Administración Electrónica (LAE), regula o acceso electrónico dos cidadáns aos Servizos Públicos como un verdadeiro dereito dos cidadáns:

Recoñéceselles aos cidadáns o dereito a relacionarse coas Administracións Públicas utilizando medios electrónicos (...), así como para obter informacións, realizar consultas e alegacións, formular solicitudes, manifestar consentimento, entaboar pretensións, efectuar pagamentos, realizar transaccións e opoñerse ás resolucións e actos administrativos. "

Entre outros, a LAE recoñécenos igualmente os seguintes dereitos:

A non volver achegar os datos e documentos que xa obren en poder das Administracións Públicas.

A coñecer por medios electrónicos o estado de tramitación dos procedementos nos que sexamos interesados.

A obter copias electrónicas dos documentos electrónicos que formen parte dos devanditos procedementos.

A dixitalización de documentos e o uso xeneralizado de Internet nos procedementos administrativos levará consigo un importante aforro do gasto público (menos papel, menos locais destinados a arquivo, menos custos de transporte, burocracia máis lixeira, trámites automatizados que reducirán os gastos extra de persoal, e un longo etcétera).

Estas vantaxes son paralelas dos igualmente importantes beneficios para o cidadán: menos gastos en desprazamentos (moitas veces inútiles) e carreiras dunha xanela a outra; aforro de tempo estragado en esperas de interminables colas; evitar o "volva vostede mañá" con horarios amplos para presentar unha solicitude ou un documento ás 12:00 dun domingo; máis comodidade, etc.

Xurden novas necesidades: a identificación e autenticación na Administración Electrónica

Ante a necesidade de concretar o disposto na LAE, adoptouse o Real Decreto 1671/2009, do 6 de novembro, polo que se desenvolve parcialmente a Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos.

Este Real Decreto, cuxo ámbito se circunscribe á Administración Xeral do Estado e os organismos públicos vinculados ou dependentes desta, ten por obxecto desenvolver a LAE en todo o relativo á transmisión de datos, sedes electrónicas e punto de acceso xeral, identificación e autenticación, rexistros electrónicos, comunicacións e notificacións e documentos electrónicos e copias.

É en concreto o Capítulo I do seu Título III o que aborda todo o relativo á identificación e autenticación no acceso electrónico dos cidadáns á devandita administración e órganos dependentes. Así, o artigo 10.1 dispón que: "As persoas físicas poderán utilizar para relacionarse electronicamente coa Administración Xeneral do Estado e os organismos públicos vinculados ou dependentes, os sistemas de sinatura electrónica incorporados ao Documento Nacional de Identidade, en todo caso, e os sistemas de sinatura electrónica avanzada admitidos".

Unha vez máis, vemos a admisión preferente do DNIe fronte a outros tipos de sinatura electrónica que, sen ser limitados estritamente á sinatura electrónica recoñecida, con todo deben ser aceptados pola administración. Isto faise patente especialmente no referente a outros sistemas de sinatura electrónica (especialmente os non criptográficos), os cales deberán aprobarse mediante Orde Ministerial ou mesmo mediante acordo do Consello de Ministros, logo de informe do Consello Superior de Administración Electrónica, sobre a base do disposto no artigo 11 do Real Decreto 1671/2009.

Este Real Decreto dispón tamén o réxime especial de habilitación para a representación de terceiros e crea o Rexistro electrónico de apoderamentos para actuar electronicamente ante a Administración Xeral do Estado e os seus organismos públicos dependentes ou vinculados, regulado no seu artigo 15.

Finalmente, o artigo 16 desenvolve a identificación e autenticación dos cidadáns, cando fose necesaria, de forma persoal ante funcionarios públicos especialmente habilitados, os cales deberán de contar cunha sinatura electrónica aceptada e estar nun rexistro especial que manterá o Ministerio da Presidencia e cuxas funcións se poderán estender a outras Administracións Públicas mediante convenio.

Isto no relativo á Administración Xeral do Estado; e que hai de Galicia?

Pois, pola súa banda, a nosa Comunidade Autónoma, aprobou recentemente o Decreto 198/2010, do 2 de decembro, polo que se regula o desenvolvemento da Administración electrónica na Xunta de Galicia e nas entidades dela dependentes. O seu Capítulo IV é o

encargado de regular todo o relativo á identificación e autenticación ante a devandita administración autonómica.

En concreto, o seu artigo 14.2 dispón que "os cidadáns poderán utilizar os seguintes instrumentos de identificación para relacionarse coa Xunta de Galicia e as entidades incluídas no ámbito de aplicación deste decreto:

En todo caso, os sistemas de sinatura electrónica incorporados ao documento nacional de identidade, para persoas físicas.

Sistemas de sinatura electrónica avanzada, incluíndo os baseados en certificado electrónico recoñecido, admitidos polas administracións públicas que teñan validez para a Xunta de Galicia e que se especifiquen na sede electrónica.

Sistemas de sinatura electrónica, como a utilización de claves concertadas nun rexistro previo como persoa usuaria inscrita no rexistro de funcionarios habilitados pola Xunta de Galicia.

Outros sistemas de identificación que resulten proporcionais e seguros para a identificación das persoas interesadas. "

Como podemos comprobar, séguese o mesmo esquema xeral da LAE e do Real Decreto, pero con rexistros propios e abrindo máis a admisibilidade doutros sistemas de identificación, observando a súa seguridade e proporcionalidade cuxa aplicación haberá que seguir na práctica.

Pola súa banda, o artigo 15.2 dispón que "A sinatura electrónica deberá cumprir as normas establecidas no protocolo de identificación e sinatura electrónica. "

O devandito protocolo deberá ser aprobado, entre outros, no prazo de un ano polo titular da consellería con competencias en materia de administracións públicas, segundo se recolle na Disposición Final Primeira do Decreto da Xunta. Polo tanto, este Decreto será desenvolvido neste punto antes de decembro de 2011.

4.5. Seguridade e interoperabilidade: os "esquemas"

Sen dúbida, outro desenvolvemento normativo de enorme importancia no ámbito da administración electrónica e, en concreto, da LAE, supóñeno os chamados "esquemas" aprobados polo Real Decreto 4/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración electrónica, e o Real Decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade, no ámbito da Administración electrónica.

Ambos os dous regulamentos abordan dous aspectos fundamentais e non sempre tomados en canta nos proxectos de administración electrónica no pasado: a seguridade e, moi especialmente, a interoperabilidade.

O primeiro deles, sen dúbida, é obvio: tendo en conta a inxente e sensible cantidade de información que atesoura a administración e que será doadamente accesible e (por que non o dicir) manipulable unha vez se dixitalice mediante sistemas informáticos, faise necesario establecer un estrito réxime de medidas de seguridade a aplicar toda a documentación pública electrónica. Isto é o que realiza o Real Decreto 3/2010 mediante a adopción do chamado "Esquema Nacional de Seguridade" (ou "ENS").

Tal e como dispón a Exposición de motivos do devandito Real Decreto:

"A finalidade do Esquema Nacional de Seguridade é a creación das condicións necesarias de confianza no uso dos medios electrónicos, a través de medidas para garantir a seguridade dos sistemas, os datos, as comunicacións, e os servizos electrónicos, que permita aos cidadáns e ás Administracións públicas o exercicio de dereitos e o cumprimento de deberes a través destes medios.

O Esquema Nacional de Seguridade persegue fundamentar a confianza en que os sistemas de información prestarán os seus servizos e custodiarán a información de acordo coas súas especificacións funcionais, sen interrupcións ou modificacións fóra de control, e sen que a información poida chegar ao coñecemento de persoas non autorizadas. Desenvolverase e perfeccionará en paralelo á evolución dos servizos e a medida que vaian consolidándose os requisitos destes e das infraestruturas que o apoian. "

Ben é certo que no noso Dereito xa contabamos cunha ferramenta de enorme utilidade a este respecto: o Real Decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei Orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal dispón no seu Título VIII un completo réxime de medidas de seguridade que deben ser adoptadas en todo sistema onde se traten datos de carácter persoal (xa sexa electrónico ou en papel). Non obstante, esta normativa resulta soamente aplicable a datos persoais e non sería aplicable a outra documentación das

administracións que non afecten á privacidade dos cidadáns.

Así, co ENS asegúrase un réxime máis amplo e adaptado aplicable a toda a documentación, datos e arquivos obrantes nas Administracións públicas. O seu artigo 1.2 dispón que o ENS "está constituído polos principios básicos e requisitos mínimos requiridos para unha protección axeitada da información. Será aplicado polas Administracións públicas para asegurar o acceso, integridade, dispoñibilidade, autenticidade, confidencialidade, trazabilidade e conservación dos datos, informacións e servizos utilizados en medios electrónicos que xestionen no exercicio das súas competencias".

Pola súa banda, o artigo 4 fixa os seguintes principios básicos do ENS e que se desenvolven ao longo de todo o seu articulado:

- Seguridade integral
- Xestión de riscos
- Prevención, reacción e recuperación
- Liñas de defensa
- Reavaliación periódica
- Función diferenciada

No referente á sinatura electrónica, o artigo 33 do ENS remítese ao seu Anexo II no relativo ás medidas de seguridade aplicables. Pola súa banda, o apartado 2 do mesmo dispón que "a política de sinatura electrónica e de certificados concretará os procesos de xeración, validación e conservación de sinaturas electrónicas, así como as características e requisitos esixibles aos sistemas de sinatura electrónica, os certificados, os servizos de selado de tempo, e outros elementos de soporte das sinaturas".

Polo tanto, estarase ao disposto na mencionada política específica para os efectos de garantir a correcta emisión, validación, conservación e uso das sinaturas electrónicas dentro da administración, tendo en conta o que supoñería un sistema inseguro a este respecto prestándose eventuais erros, suplantacións e inconsistencias dun sistema documental público que debería ser robusto co fin de garantir a súa plena eficacia xurídica.

A interoperabilidade é, se cabe, tan ou máis necesaria que a seguridade posto que é a gran materia pendente da Administración electrónica ata a lexislación actual: referímonos á necesidade de que os datos de todas as administracións poidan cruzarse e interrelacionarse cos obrantes noutras entidades, sempre de acordo coa Lei, sen crear "reinos de Taifas" ou sistemas illados que son incapaces de comunicarse ou, se o fan, é con grandes dificultades e demoras inxustificadas. Por outro lado, os sistemas públicos non deben discriminar os cidadáns en función da súa elección tecnolóxica, debendo ser amplamente

compatibles con todas as plataformas informáticas do mercado. O seu réxime desenvólvese no Real Decreto 4/2010 que regula o chamado "Esquema Nacional de Interoperabilidade" (ou ENI).

A súa Exposición de Motivos afirma que "a finalidade do Esquema Nacional de Interoperabilidade é a creación das condicións necesarias para garantir o axeitado nivel de interoperabilidade técnica, semántica e organizativa dos sistemas e aplicacións empregados polas Administracións públicas, que permita o exercicio de dereitos e o cumprimento de deberes a través do acceso electrónico aos servizos públicos, á vez que redunda en beneficio da eficacia e a eficiencia,".

Así, o seu artigo 1.2 dispón que o ENI "comprenderá os criterios e recomendacións de seguridade, normalización e conservación da información, dos formatos e das aplicacións que deberán ser tidos en conta polas Administracións públicas para asegurar un axeitado nivel de interoperabilidade organizativa, semántica e técnica dos datos, informacións e servizos que xestionen no exercicio das súas competencias e para evitar a discriminación aos cidadáns por razón da súa elección tecnolóxica".

Tal e como o facía o ENS, o artigo 4 do ENI establece os seguintes principios básicos que guían a regulación da interoperabilidade:

- A interoperabilidade como calidade integral.
- Carácter multidimensional da interoperabilidade.
- Enfoque de solucións multilaterais.

No referente á interoperabilidade de sinatura electrónica e de certificados, o artigo 18 do ENI dispón o seguinte:

> "1. A Administración Xeral do Estado definirá unha política de sinatura electrónica e de certificados que servirá de marco xeral de interoperabilidade para a autenticación e o recoñecemento mutuo de sinaturas electrónicas dentro do seu ámbito de actuación. Non obstante, a devandita política poderá ser utilizada como referencia por outras Administracións públicas para definir as políticas de certificados e sinaturas a recoñecer dentro dos seus ámbitos competenciais. (…)

5. A política de sinatura electrónica e de certificados, mencionada no apartado primeiro do presente artigo, establecerá as características técnicas e operativas da lista de prestadores de servizos de certificación de confianza que recollerá os certificados recoñecidos e interoperables entre as Administracións públicas e que se consideren fiables para cada nivel de aseguramento concreto, tanto no ámbito nacional como europeo. A lista que estableza a Administración Xeral do Estado poderá ser utilizada como referencia por outras

Administracións públicas para definir as súas listas de servizos de confianza para aplicación dentro dos seus ámbitos competenciais. "

Neste sentido, preténdese garantir o establecemento de criterios comúns de recoñecemento e interoperabilidade dos distintos sistemas de sinatura electrónica utilizados e aceptados no seo das administracións públicas: tanto por parte dos cidadáns e entidades coma polas propias administracións e organismos.

5.

A SINATURA ELECTRÓNICA EN CIFRAS

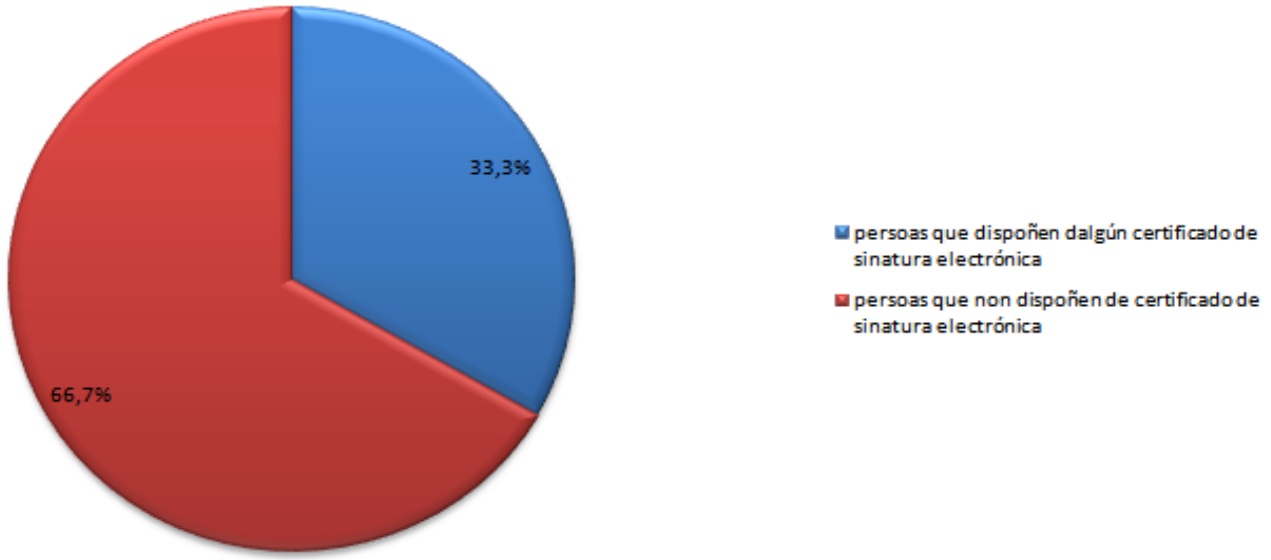
A continuación faise unha breve análise dalgúns indicadores relacionados coa certificación dixital e a sinatura electrónica y danse algunhas pinceladas sobre a relación destes indicadores co contexto tecnolóxico existente na actualidade en España e Galicia.

Para o desenvolvemento deste apartado utilizáronse como fontes datos procedentes tanto do *Instituto Nacional de Estadística* como do Observatorio da Sociedade da Información e a Modernización de Galicia e hai que ter en conta que os datos incluídos no mesmo, sempre que non se indique o contrario, refírense ao mes de xaneiro do ano referido.

CIDADÁNS

Na actualidade dos 34,6 millóns de persoas residentes en España, de entre 16 e 74 anos, aproximadamente o 27,5% dispón xa de DNI electrónico e só o 9% dispón doutros tipos de certificados de sinatura electrónica recoñecidos.

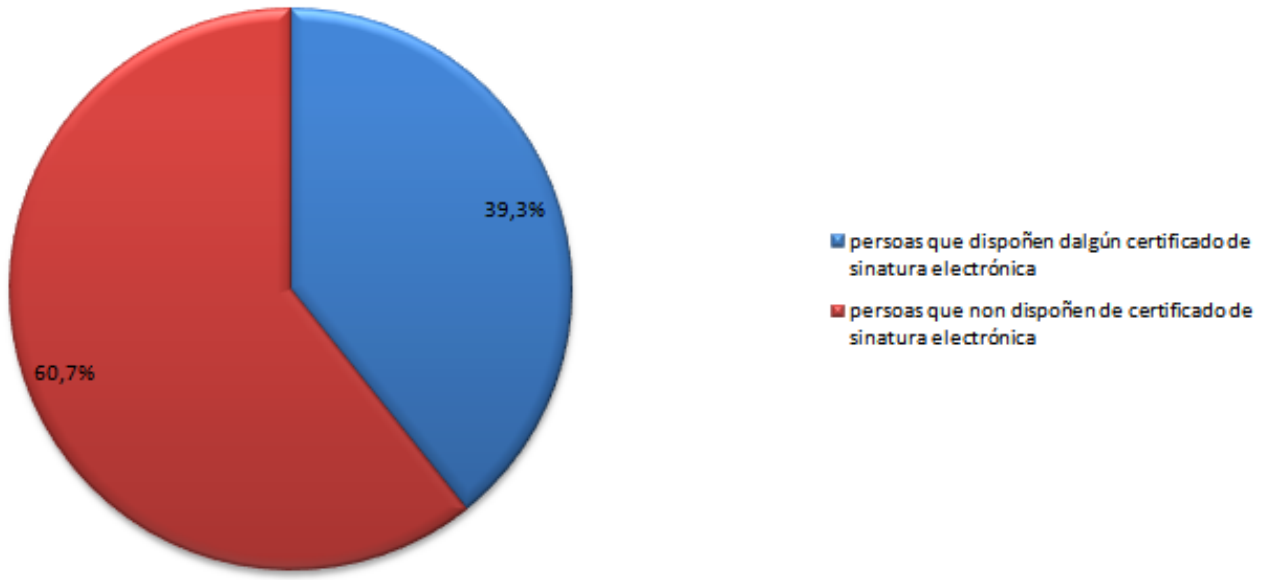
Algo máis de 11,5 millóns de persoas, é dicir aproximadamente un 33% da poboación, dispoñen actualmente dalgún certificado de sinatura electrónica. Isto supón que actualmente en España algo máis de 23 millóns de persoas non teñen ningún tipo de certificado de sinatura electrónica recoñecido. Cabe destacar que hai aproximadamente 100.000 persoas residentes en España, pero de nacionalidade estranxeira, que dispoñen actualmente de certificados de sinatura electrónica recoñecidos.



Gráfica1: Dispoñibilidade dalgún certificado de sinatura electrónica en España. Ano 2010.

BASE: persoas residentes en España de entre 16 e 74 anos.

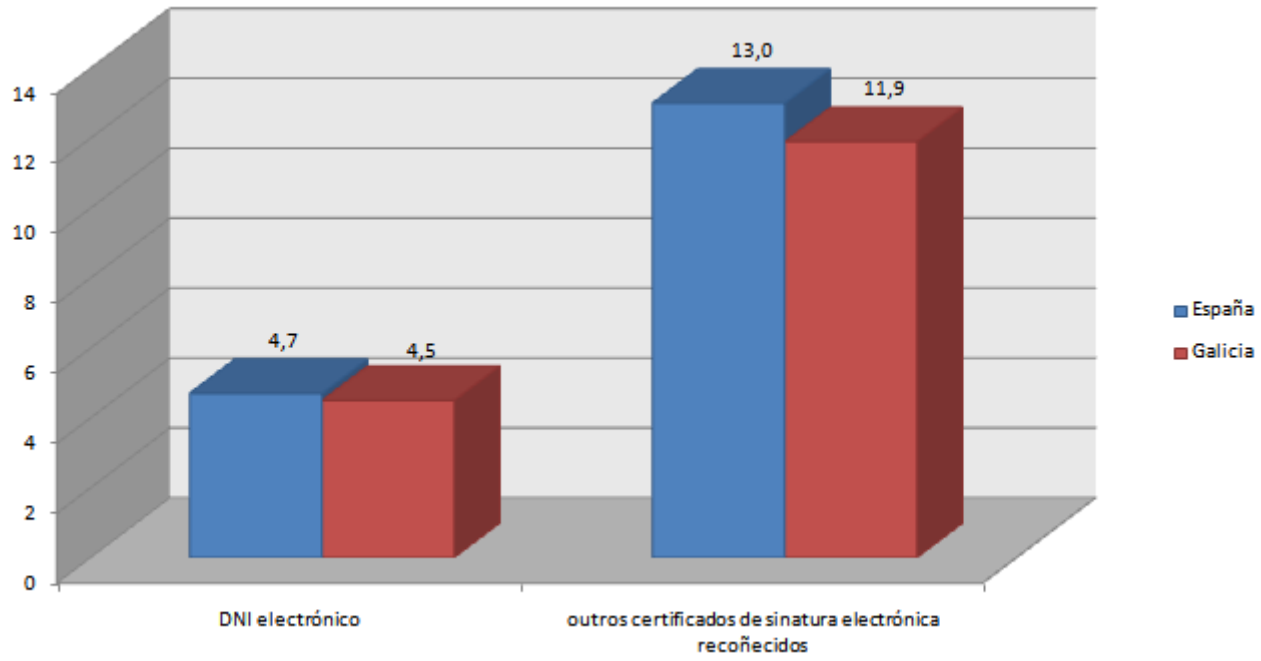
En Galicia, a porcentaxe de persoas que dispoñen dalgún certificado de sinatura electrónica é superior á media de España, e sitúase algo por enriba do 39% da poboación (aproximadamente 800.000 persoas).



Gráfica2: Dispoñibilidade dalgún certificado de sinatura electrónica en Galicia. Ano 2010.

BASE: persoas residentes en Galicia de entre 16 e 74 anos.

Un 4,7% das persoas residentes en España de entre 16 e 74 anos de idade utilizaron o DNI electrónico durante o último ano para as súas relacións coas Administracións públicas e o 13% utilizou outros certificados de sinatura recoñecidos. Como pode verse na seguinte gráfica, en Galicia estes datos de utilización son lixeiramente inferiores, tanto no caso do DNI electrónico coma no caso doutros certificados de sinatura electrónica recoñecidos.



Gráfica3: Utilización de certificados de sinatura electrónica para as relacións coas Administracións Públicas, en Galicia e España. Ano 2010.

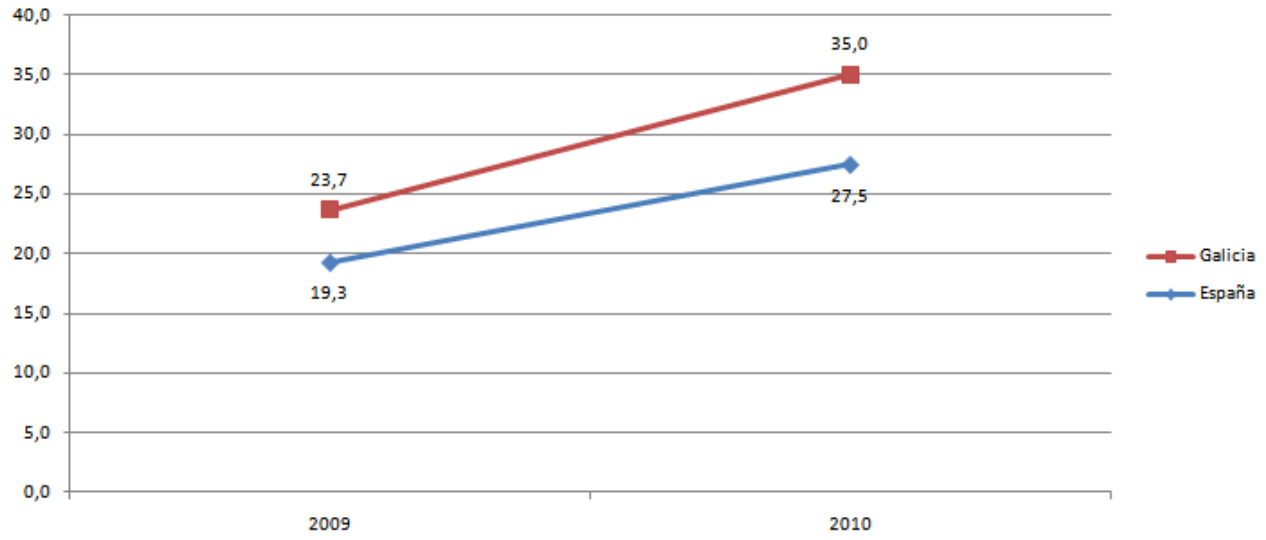
BASE: persoas residentes en Galicia e España de entre 16 e 74 anos.

Dos datos anteriores conclúese que, en xeral, se ben o DNI electrónico é, con diferenza, o dispositivo de sinatura electrónica máis estendido entre os cidadáns aínda.

Cabe destacar, porén, que existe un segmento de poboación, o formado polas persoas que aínda están a realizar estudos, no que para a relación coas Administración Públicas se utilizou máis o DNI electrónico que calquera outro dispositivo.

É significativo destacar neste punto o dato relativo á dispoñibilidade do DNI electrónico en Galicia que, cunha porcentaxe do 35% da poboación, é actualmente moi superior á media en España (7,5 puntos porcentuais máis).

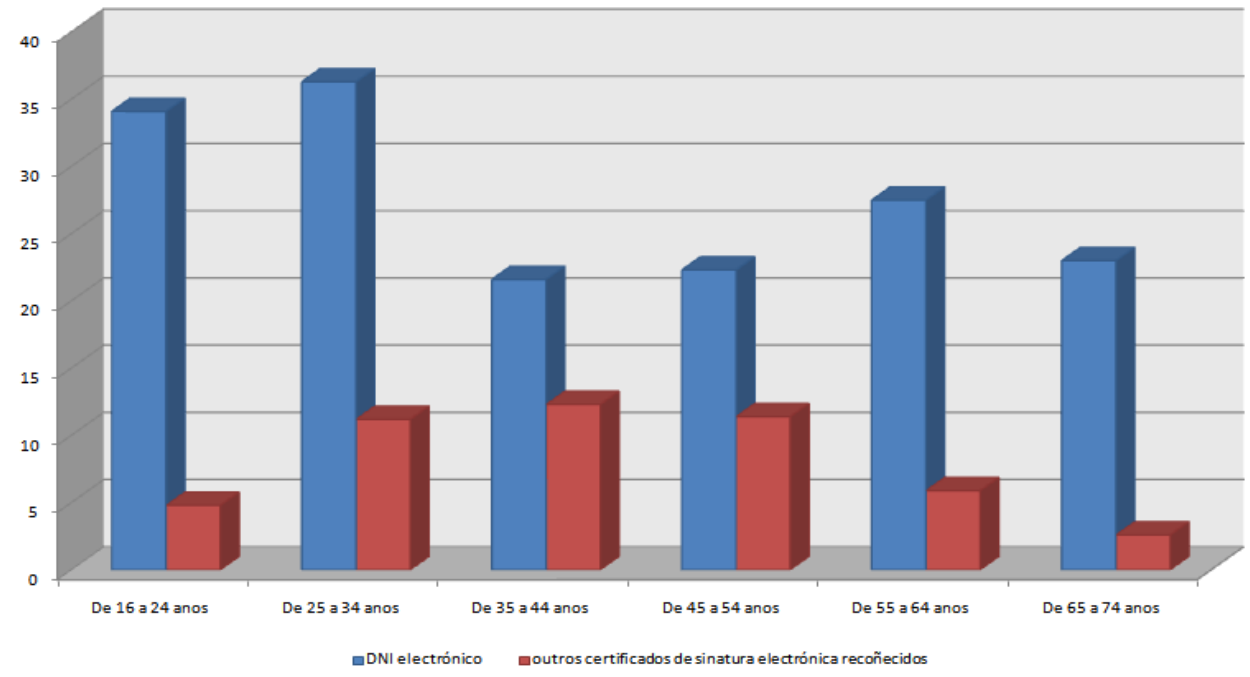
Hai que destacar, tamén neste sentido, que o incremento en Galicia da dispoñibilidade do DNI electrónico se situou durante o último ano ao redor do 48%, pasando do 23,7% no ano 2009 ao 35% no ano 2010.



Gráfica4: Evolución da dispoñibilidade do DNI electrónico en Galicia e España. Anos 2009-2010.

BASE: total de persoas residentes en Galicia e España de entre 16 e 74 anos.

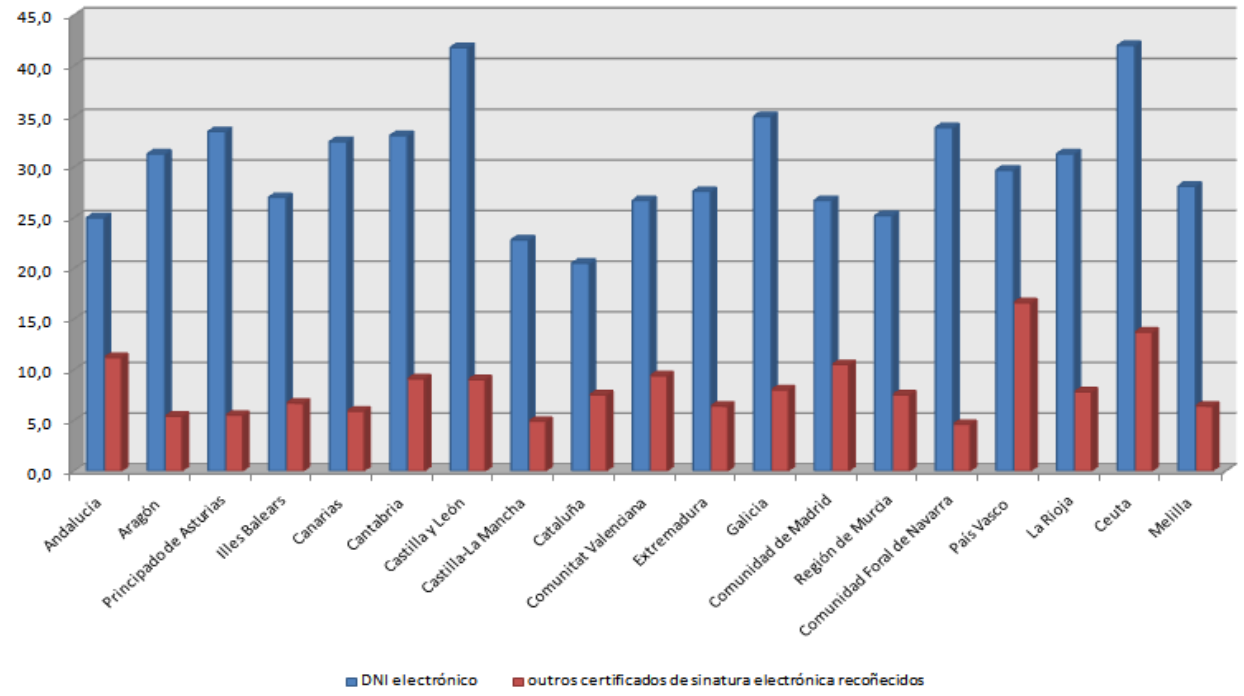
Na seguinte figura móstrase, de xeito agrupado por rango de idade, a disposición de DNI electrónico e doutro tipo de certificados por parte dos cidadáns:



Gráfica5: Dispoñibilidade de certificados de sinatura electrónica (DNI electrónico e outros)

BASE: total de persoas residentes en España de entre 16 e 74 anos.

Por comunidades autónomas, como pode apreciarse na seguinte táboa, a dispoñibilidade do DNI electrónico varía entre case o 42% de Castela e León e Ceuta e o escaso 20% de Cataluña. No caso doutros certificados de sinatura electrónica recoñecidos a dispoñibilidade varía entre o 16,6% no País Vasco e o 4,6% da Comunidade Foral de Navarra.



Gráfica6: Dispoñibilidade de certificados de sinatura electrónica (DNI electrónico e outros)

BASE: total de persoas residentes en España de entre 16 e 74 anos.

Resulta sorprendente, á vista dos datos anteriores, que comunidades autónomas con entidade de certificación propia, como Cataluña ou a Comunidade Valencia, non despunten de xeito destacado sobre o resto de autonomías en canto á dispoñibilidade de certificados de sinatura electrónica recoñecidos dos seus cidadáns. Con todo, a dispoñibilidade de certificados de sinatura electrónica, diferente ao DNI electrónico, no País Vasco (outra das comunidades con entidade de certificación) se é significativamente maior cá media.

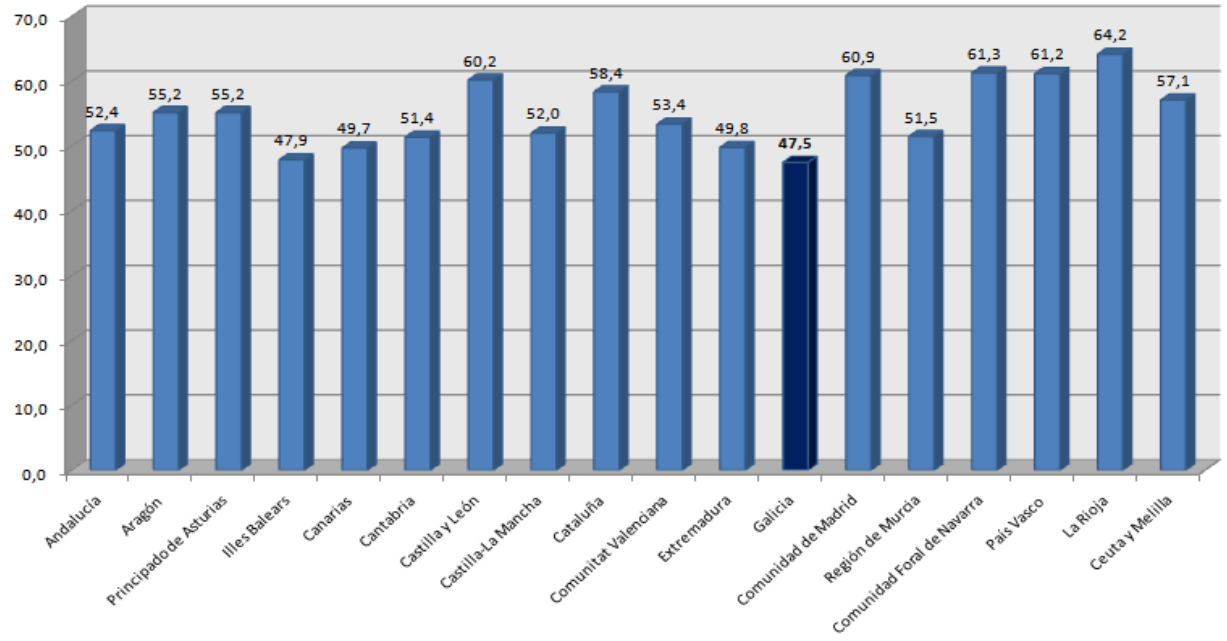
A continuación detállanse algúns datos significativos que axudan a contextualizar o ámbito tecnolóxico actual, da poboación de Galicia e España:

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

EMPRESAS DE 10 E MÁIS EMPREGADOS

En España o 55,7% das empresas en España de 10 e máis empregados con conexión a Internet utilizou sinatura electrónica nalgunha comunicación enviada durante o último ano dende a súa empresa.

Este dato da utilización da sinatura electrónica para comunicacións enviadas por empresas de 10 ou máis empregados, analizado por Comunidade Autónoma, móstrase no seguinte gráfico:

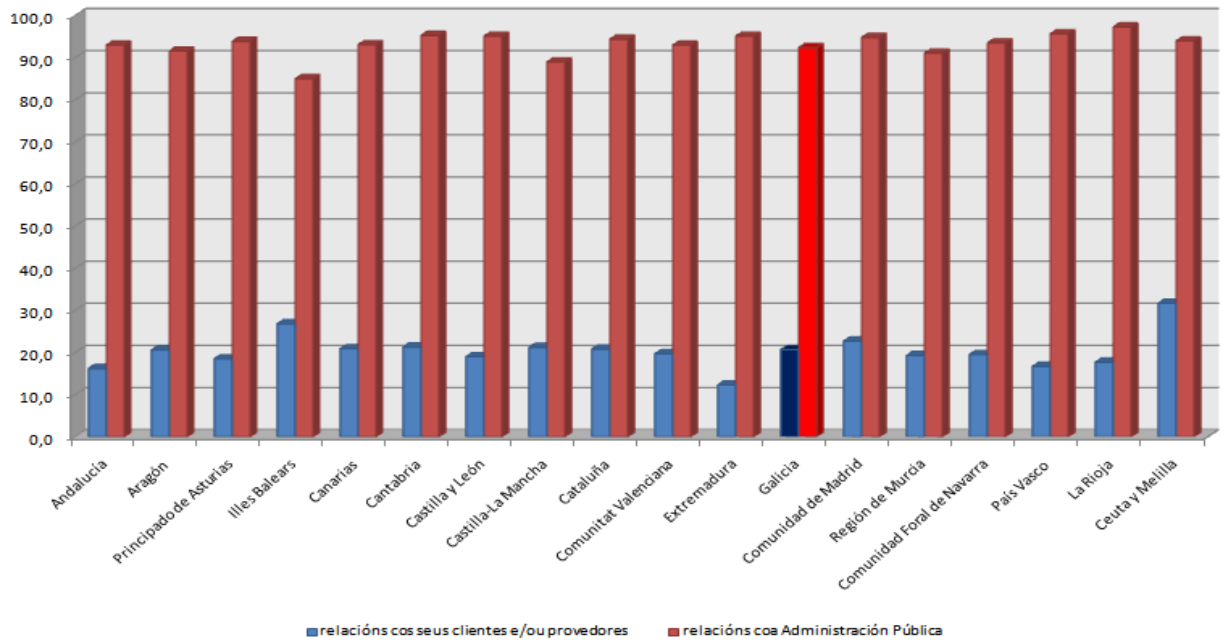


Gráfica7: Utilización de sinatura electrónica nalgunha comunicación enviada durante o último ano

BASE: empresas de 10 e máis empregados con conexión a Internet. Ano 2010.

Como pode apreciarse, o grao de utilización da sinatura electrónica por parte das empresas varía substancialmente entre as diferentes comunidades autónomas e se sitúa entre o 64,2% de A Rioxa e o 47,5% de Galicia, que neste aspecto se sitúa moi por debaixo da media en España.

Prácticamente a totalidade das empresas (93,5%), que utilizaron sinatura electrónica nalgunha comunicación enviada durante o último ano, empregouna para relacionarse coa Administración Pública mentres que só un 20% o fixo para relacionarse cos seus clientes e/ou provedores.

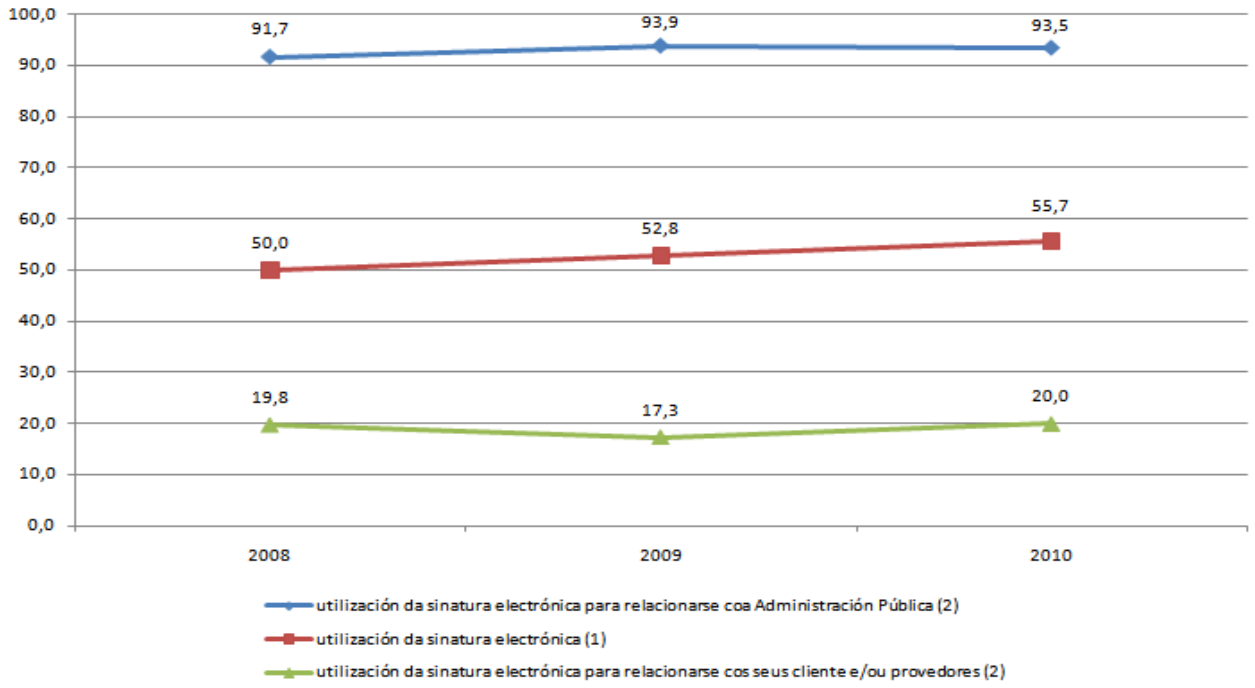


Gráfica8: Utilización de sinatura electrónica nalgunha comunicación enviada durante o último ano

BASE: empresas de 10 e máis empregados con conexión a Internet que utilizou sinatura electrónica nalgunha comunicación enviada. Ano 2010.

Como pode apreciarse na gráfica, en todas as Comunidades Autónomas, sen excepción, a utilización da sinatura electrónica por parte das empresas para as relacións coas Administracións Públicas é significativamente maior que para as relacións cos seus clientes e provedores.

Como pode observarse no gráfico seguinte nos últimos anos produciuse un avance moderado na utilización por parte das empresas da sinatura electrónica.



Gráfica9: Evolución da utilización por parte das empresas da sinatura electrónica

BASE (1): empresas de 10 e máis empregados con conexión a Internet. Ano 2010.

BASE (2): empresas de 10 e máis empregados con conexión a Internet que utilizou sinatura electrónica nalgunha comunicación enviada. Ano 2010.

A continuación detállanse algúns datos significativos que axudan a contextualizar o ámbito tecnolóxico actual en Galicia e no conxunto do Estado:

INDICADORES TECNOLÓXICOS	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%
Empresas con correo electrónico	94,7%	90,6%	96,5%	94,5%
Porcentaxe de empresas que realizaron intercambio electrónico de datos entre empresas	36,7%	33,6%	45,0%	39,6%
Porcentaxe de empresas que realizaron intercambio electrónico de datos mediante envío de pedidos aos seus provedores [1]	21,5%	20,3%	51,2%	56,3%

INDICADORES TECNOLÓXICOS	2009		2010	
	España	Galicia	España	Galicia
Porcentaxe de empresas que realizaron intercambio electrónico de datos mediante recepción de facturas electrónicas [1]	41,0%	26%	51,2%	58,8%
Porcentaxe de empresas que realizaron intercambio electrónico de datos mediante recepción de pedidos de clientes [1]	17,0%	17,2%	19,3%	17,8%
Porcentaxe de empresas que realizaron intercambio electrónico de datos mediante envío de facturas electrónicas [1]	23,1%	19,2%	25,1%	22,8%
Porcentaxe de empresas que realizaron intercambio electrónico de datos mediante envío ou recepción de información sobre produtos [1]	57,4%	61%	63,1%	63,9%
Porcentaxe de empresas que realizaron intercambio electrónico de datos mediante envío ou recepción de documentación sobre transporte, envíos ou entregas [1]	42,9%	44,5%	50,5%	53,6%
Porcentaxe de empresas que realizaron intercambio electrónico de datos mediante envío de instrucións de pagamento a entidades bancarias [1]	75,5%	72,9%	74%	71,5%
Porcentaxe de empresas que realizaron intercambio electrónico de datos mediante intercambio automatizado de información coa AAPP [1]	60,0%	59,9%	56,6%	57,5%
Porcentaxe de empresas que compartían electronicamente información cos seus provedores ou clientes da cadea de subministración	14,2%	13,7%	17,6%	15%

[1] Porcentaxe sobre o total de empresas que realiza intercambio electrónico de datos

6.

OS RETOS DO FUTURO NA IDENTIDADE DIXITAL

DIVULGACIÓN, FORMACIÓN E USABILIDADE

Nos últimos anos estanse a levar a cabo labores de divulgación e formación sobre os beneficios e utilización dos certificados electrónicos.

O Ministerio de Industria, Turismo e Comercio trata de fomentar o uso do DNIe impartindo sesións formativas presenciais, onde se aborda unha parte teórica que se complementa cunha sesión formativa en liña. Estas sesións son gratuítas e abonda con inscribirse previamente a través dun formulario web en www.formacionDNI.es. Nestas xornadas ten especial importancia transmitir ao cidadán os procedementos de xeito sinxelo e claro.

A Administración Pública debe asumir o reto da mellora continua para a implantación do DNIe, e mirar cara a outros países onde a emisión do certificado electrónico de cidadán é acompañada por servizos de formación, axuda e mesmo provisión dun lector de cara a facilitar e promover o seu uso dende o momento da emisión.

Por outra parte, este labor de formación, divulgación e asesoramento estase a levar a cabo tamén no ámbito empresarial, en gran parte polos prestadores de servizos de certificación electrónica. Contar cunha estratexia de apoio clara por parte da Administración Pública será importante para potenciar este reto de transmitir os beneficios e aforro de custos que achega ás organizacións a utilización da certificación electrónica, actualizando como catalizador do devandito proceso. No actual escenario de crise cada punto de mellora por pequeno que sexa é importante, e a utilización da sinatura electrónica de cara á optimización de procesos pode ser unha das claves para a mellora da produtividade.

Pero paralelas ás necesidades anteriormente descritas existe unha moi importante: a usabilidade. Poderiamos dicir que o certificado debería chegar a ser "invisible", entendendo como tal que o seu uso debe ser doado, natural e case transparente para os cidadáns. Neste reto xogan un papel relevante factores como o dispositivo que contén o certificado, a súa compatibilidade, as aplicacións ou os operadores de comunicacións entre outros, e un dos retos é que terán que traballar de xeito coordinado no futuro para alcanzar os devanditos obxectivos.

O feito de que sexamos quen de converter os cidadáns en e-cidadáns dependerá en boa medida de que a administración electrónica sexa unha realidade e que as empresas ofrezan os seus servizos na rede coas mesmas condicións, garantías e seguridade que no seu modelo tradicional.

INTEROPERABILIDADE E ESTANDARIZACIÓN

Nun escenario global de eliminación de barreiras tecnolóxicas e físicas non se entende o uso de sistemas illados, que traballen de xeito autónomo. A certificación electrónica non

pode ser unha excepción e débese prestar especial importancia a que todos os dispositivos e sistemas sexan interoperables e se baseen na utilización de estándares. Isto permitiranos por unha parte manter a neutralidade tecnolóxica e por outra abrir as nosas fronteiras electrónicas a Europa nun principio e ao resto do mundo despois.

Dende un punto de vista técnico a converxencia tecnolóxica de dispositivos facilitará este labor, e paralelo a iso os sistemas de información evolucionarán cara á utilización de formatos abertos como XML ou XADES-XL, permitindo a correcta identificación e codificación de campos e atributos, e cara á compatibilidade sintáctica ou semántica coa utilización de repositorios sincronizados, dotando todo iso ás solucións dun gran valor engadido.

A nivel de relacións comerciais España debe estar interesada en conseguir esta interoperabilidade canto antes, sobre todo tendo en conta o papel de liderado que neste sector ocupa España e as posibilidades de negocio que se abren fóra das nosas fronteiras, sobre todo cos países latinoamericanos.

Nun escenario a longo prazo é interesante seguir a evolución do proxecto **STORK** que permitirá conseguir o recoñecemento paneuropeo das identidades electrónicas, e en concreto a aceptación do DNI electrónico e identificadores similares en servizos de Administración electrónica doutros Administracións europea.

RETOS LEXISLATIVOS

O principal reto ao que se enfronta a nosa lexislación é a plena adaptación de esta aos novos medios dixitais, sen poñer trabas ou requisitos formais innecesarios para a xeneralización e plenos recoñecemento dos documentos dixitais na totalidade do tráfico xurídico, tanto no ámbito público coma no privado.

A proverbial (e, ás veces, necesaria) lentitude do Dereito á hora de adaptarse e regular as novas realidades convértese nun verdadeiro lastre no vertixinoso mundo tecnolóxico de hoxe en día. A nova sociedade dixital demanda solucións áxiles e dinámicas que acheguen seguridade xurídica aos millóns de transaccións que se dan todos os días en Internet.

A nosa capacidade produtiva e competitiva depende diso neste novo escenario tan cambiante e globalizado.

A vertixe que poidamos sentir ante o descoñecemento das novas tecnoloxías e a inseguridade que instintivamente sentimos ante o que non podemos tocar e ulir non debe facernos caer en impoñer máis esixencias ao mundo virtual das que xa aplicamos no mundo físico. Desgraciadamente, moita da nosa normativa actual é mostra patente diso como, por exemplo, a nosa actual regulación da factura electrónica cuxos requisitos superan con

moito aos aplicables á factura en papel e aínda moito máis aos que se piden na práctica respecto a estas últimas. Na nosa opinión, a devandita lexislación debe alixeirarse e flexibilizarse sen perder nunca de vista os criterios e principios de interoperabilidade e de neutralidade tecnolóxica que comentamos anteriormente.

É posible lograr unha seguridade xurídica suficiente no mundo dixital sen poñer trabas innecesarias e/ou excesivas aos suxeitos que deciden utilizalo como principal ou mesmo único medio de operar no mercado e na sociedade actual.

O futuro, sen dúbida, demándanolo.

SEGURIDADE

O incremento no uso das comunicacións a través de internet tanto nas relacións persoais coma nas comerciais leva consigo uns riscos que se deben minimizar. De feito a inseguridade é un das grandes barreiras á utilización profesional e comercial de internet, e co impulso que están a tomar as redes sociais podrecía selo tamén a nivel persoal.

A utilización de elementos como o certificado electrónico persoal ou profesional, o certificado de sede electrónica ou calquera mecanismo que garanta que a entidade ou a persoa que está ao outro lado é quen di ser e ademais é segura, promoven e fortalecen a utilización de transaccións comerciais a través da rede. Neste proceso confluén múltiples actores, dende o fabricante dos dispositivos que albergan o certificado, as autoridades de certificación que levan a cabo a validación e os provedores de servizo ou fabricantes de *software*, sen que se nos esquece o papel que ocupa a Xustiza na definición dun marco legal en continua adaptación que regula a participación das devanditas entidades.

É importante destacar que no ámbito de seguridade o certificado electrónico non é un mecanismo ou solución exclusiva senón que achega un valor engadido importante en ámbitos que o complementan con outros elementos, por exemplo biométricos, para dotar ás solucións dos máis esixentes niveis de seguridade.

No ámbito da seguridade o INTECO desenvolveu unha iniciativa moi interesante para ofrecer á industria un esquema de certificación contra unha norma nacional e internacional de requisitos de seguridade que permitise que as aplicacións e servizos que se certifiquen contra os devanditos perfís dispuxesen de maiores garantías de seguridade e confianza. As aplicacións que se desenvolvan apoiándose nestes perfís poden, por un lado, dispoñer de mellores requisitos de seguridade e, por outro lado, levar a cabo un proceso formal de avaliación e certificación contra os devanditos perfís, obtendo un certificado de nivel Common Criteria que lles achegue tamén un selo de calidade e unha ferramenta máis de competitividade. Así mesmo outras aplicacións ou servizos que se apoien en sinatura

electrónica ou dixital poden tamén seguir procesos de certificación similares e elevar o seu nivel de seguridade así como a súa imaxe cara ao exterior gañando confianza no sector que vai usar as devanditas aplicacións.

CONVIVENCIA DAS ENTIDADES PÚBLICAS E PRIVADAS

A oferta e demanda funcionan habitualmente como regulador dos mercados, pero necesítanse unha serie de normas que sexan de obrigado cumprimento e cuxa aplicación evite conflitos de intereses que impidan ou atrasen a evolución das certificacións electrónicas nun mercado global.

Cando o DNIe despegue ocupará posiblemente o oco de certificado de cidadán e desprazará ao doutras entidades, co que poderiamos dicir que a longo prazo tería sentido que desaparecesen as iniciativas públicas ou privadas de expedir identidades dixitais persoais. O DNIe é un servizo capaz de xestionar a maior parte das necesidades de identificación a nivel persoal e curiosamente o sector privado non o ve como unha ameaza, senón como un habilitador ou dinamizador do proceso.

Con todo, a nivel empresarial o certificado de profesional cubrirá as necesidades dos profesionais, asociados ou empresas para as que non serve o DNIe. Aí é onde se centrará con total seguridade o desenvolvemento do negocio das entidades de certificación privadas, e mesmo o da FNMT. Se garantimos o cumprimento da lexislación que establece as obrigas e responsabilidades dos prestadores de servizos de certificación e a súa propia certificación, deberían poder convivir ambos os dous tipos de entidades de xeito armónico e velando por uns intereses comúns.

FACTURACIÓN E ADMINISTRACIÓN ELECTRÓNICA

Se falamos de sistemas de información e certificación electrónica existen dous puntos de encontro que non podemos escusar, trátase da facturación electrónica e da contratación electrónica en Administración Pública. Quizais vexamos lonxe un nivel alto na implantación e consolidación destas tecnoloxías, pero dende logo será un salto cualitativo moi importante de cara a mellorar a produtividade en España.

O sector industria demanda unha facturación electrónica integrada cos sistemas de información das canles de produción, almacenamento e loxística, que permita en tempo real ter o control do seu negocio. Este cambio gradual levaría consigo un aforro de custos de almacenamento e seguramente a orientación das empresas de fabricación á utilización de metodoloxías e procesos de produción "*just in time*" coas conseguintes vantaxes de produtividade da que xa falamos.

Por outra parte, os procesos da Administración Pública poderían orientarse a fluxos de traballo integrados dende o inicio ata o fin cos cidadáns e as empresas, que lles permitan garantir a integridade, transparencia e seguridade dos seus procedementos. Ademais, a calidade do servizo percibido polos usuarios incrementaríase considerablemente posto que permitiría a igualdade de servizos independentemente do lugar de residencia ou a alta dispoñibilidade dos servizos de Administración Pública as vinte e catro horas do día e os sete días da semana.

Este reto podería aplicarse a outros sistemas de información relacionados coa certificación electrónica, e cuxo obxectivo común cos dous que detallamos será sempre a optimización e mellora de procesos tanto produtivos coma organizativos.

7. CONCLUSIÓNS

CERTIFICADOS DIXITAIS

A certificación electrónica é fundamentalmente un tema de **confianza e seguridade**. A certificación electrónica permite **realizar a través de Internet todo tipo de trámites de xeito seguro** garantindo a verdadeira identidade do usuario e permite a sinatura electrónica de documentos coa mesma validez legal que se se asinasen de puño e letra en papel. A tramitación en liña permite aos usuarios realizar multitude de xestións durante 24 horas ao día, evitando desprazamentos e esperas e xerando aforro de tempo, intermediarios, erros, arquivo físico e gastos de transporte.

Actualmente, os cidadáns que utilizan a sinatura electrónica teñen claro o seu valor de seguridade pero, en xeral, os cidadáns aínda non perciben con claridade a súa utilidade nin a súa eficacia. Un dos principais motivos do pouco uso da sinatura electrónica e do certificado dixital débese ao descoñecemento que hai das súas posibilidades e garantías, tanto a nivel empresarial coma na cidadanía.

Hai que ter en conta, ademais, que a coñecida como alfabetización dixital é aínda escasa entre a poboación, e as dificultades de comprensión destas tecnoloxías e o estado aínda incipiente da "vida dixital" fan necesaria unha optimización das aplicacións de cara a un uso amigable e compatible con todos os sistemas. Débese conseguir que o uso dos certificados dixitais sexa tan doado e transparente que se faga invisible para o cidadán.

A **estratexia de despregamento dos certificados electrónicos** debe estar en función dos proxectos que xurdan e da propia demanda, é dicir, non se deben crear necesidades artificiais de certificados electrónicos senón adaptar estes á demanda e ás necesidades reais existentes. Hai que facer unha formulación axeitada de para qué vale a certificación dixital e a sinatura electrónica e en que ámbitos ten sentido a súa utilización, poñendo por diante do despregamento de certificados e tarxetas o desenvolvemento dos sistemas de información que os necesitan. Serán o propio mercado e os usuarios os que marcarán a tendencia en todas as solucións e os retos futuros.

UTILIZACIÓN DOS CERTIFICADOS DIXITAIS

Actualmente a utilización da certificación electrónica en España está, con diferenza, **máis estendida na Administración Pública que na empresa privada**, sendo a Axencia Tributaria o organismo referente ata o momento polo uso dos certificados para a realización da Declaración da Renda.

Existe unha diferenza moi importante entre Europa e España no uso do certificado dixital xa que, mentres que en Europa o motor de promoción desta tecnoloxía foi a empresa privada (fundamentalmente a banca), en España foi a Administración Pública, en especial

,como xa se comentou, a Axencia Tributaria e, en menor medida, as cámaras de comercio e os colexios profesionais.

Dentro da Administración Pública existen diferentes graos de implantación pero, en xeral, nestes últimos anos, desenvolveuse un esforzo moi importante por modernizar e axilizar os trámites telemáticos na maioría de comunidades autónomas e en moitas corporacións locais. O escenario actual de crise económica supuxo un parón nos avances nesta materia que tivesen sido maiores, cuantitativa e cualitativamente falando, nunha situación económica normal.

Sen dúbida, as empresas privadas seguen un ritmo bastante máis lento na adopción da sinatura electrónica cás Administracións Públicas. Isto pode deberse a que **o retorno do investimento realizado en materia de certificación electrónica é un retorno "non inmediato"**. As Administracións Públicas móvense polo interese de prestar máis e mellores servizos aos cidadáns e miden o retorno do investimento en parámetros como seguridade ou beneficios sociais. Non obstante, é probable que a percepción de calidade e seguridade deste tipo de sistemas por parte dos usuarios comprometa as empresas privadas, que queren coidar a súa imaxe, a ofrecer servizos máis seguros a través de Internet utilizando este tipo de certificados.

Cando a Administración Pública remate de implantar todos os seus sistemas, as súas sedes electrónicas, factura electrónica... será o momento en que se obrigue os seus provedores a usar certificados dixitais e aos cidadáns a usar, por exemplo, o DNIe.

Un paso importante que se debería abordar dende o sector é axudar á empresa privada, á Administración Pública e a cidadanía a distinguir sobre a gran variedade de tipos de certificados dixitais existentes na actualidade: con uso limitado aos trámites coas Administracións Públicas, certificados de atributo para o mundo empresarial para asinar documentos, certificados vinculando o traballador a unha empresa cun cargo determinado nesta, DNIe,…

DNIe

É moi destacable, no panorama actual, a funcionalidade achegada polo DNIe na certificación dixital, como un dispositivo seguro que lle facilita ao cidadán a realización de trámites con total seguridade. **Este proxecto de identidade dixital é pioneiro en Europa** e serviu como referencia a outros países que comezan agora con proxectos similares, apoiándose no coñecemento xerado pola experiencia española.

A implantación definitiva do DNIe supoñerá, a medio ou longo prazo, o fin dos certificados de cidadán que a maioría dos provedores de servizos de certificación emiten actualmen-

te.

O DNIe será unha **grande axuda de cara ao cidadán aínda que é evidente que necesita mellorar a súa usabilidade**. O DNIe ten o inconveniente, que supón unha barreira que aínda hai que superar, de necesitar un lector do que non todos os ordenadores dispoñen. Esta razón, xunto coa escasa información que se ofreceu á cidadanía sobre o seu uso, é un dos principais aspectos polas que hoxe en día non todo o mundo ten acceso ou coñecemento para realizar operacións co DNIe.

UNIFICACIÓN DE DISPOSITIVOS

O futuro da certificación dixital pasa, entre outras cousas, por **unificar dispositivos e definir usos e funcións**. Se realmente se quere converter o cidadán nun cidadán dixital é necesario realizar unha converxencia de dispositivos unificando todos os dispositivos nun só, manexable e comprensible.

e-ADMINISTRACIÓN

Os grandes avances tecnolóxicos que se produciron nos últimos anos póñense, mediante a e-administración, a disposición da cidadanía e do día a día da Administración Pública. A tecnoloxía chega actualmente a todas as partes e os propios cidadáns son cada vez máis esixentes para que a propia administración ofreza servizos telemáticos.

Non obstante, **os cidadáns teñen que percibir a e-administración como unha realidade que é vantaxosa** e que lles vai proporcionar mellores relacións coa administración. Se a administración ofrece servizos importantes para o usuario a través de Internet seguro que o cidadán vai utilizalos. Hai que ter en conta, ademais, que actualmente calquera cidadán pode esixir que calquera procedemento estea en Internet.

Aínda que poida parecer que hoxe en día a certificación electrónica se limita a trámites moi concretos, hai que ter en conta que, como sucedeu noutros aspectos, todo proceso novo comeza de xeito similar e primeiro se automatizan e modernizan aqueles 4 ou 5 trámites que supoñen o 80 por cento dos servizos prestados aos cidadáns e, posteriormente, automatízanse centos deles que dan lugar ao 20 por cento residual. Nestes momentos **a maioría de comunidades autónomas e concellos grandes e medios encóntranse nunha fase de despregamento da e-administración xa bastante avanzada**, tendendo a unha consolidación desta. Pola contra, son os pequenos concellos os que se encontran nunha posición máis retraída neste sentido.

Hai que ter en conta que **a implantación electrónica necesita ir sempre ao mesmo tempo cá implantación de infraestruturas**. Neste sentido, moitas comunidades autónomas defini-

ron de xeito acertada unha estratexia de infraestruturas (banda larga,…) que favorece a implantación dos servizos dixitais especialmente nos municipios con maiores dificultades.

Aínda que o cumprimento completo e exhaustivo da Lei 11/2007 é moi difícil e supón un proceso lento, as comunidades autónomas avanzaron de xeito notable nos últimos meses na súa adaptación a esta.

Na actualidade **as barreiras á administración electrónica veñen impostas pola usabilidade das propias tecnoloxías e polo cambio cultural e de hábitos** que esta nova administración require.

INTEROPERABILIDADE

O futuro da certificación electrónica pasa pola **interoperabilidade real dentro da Unión Europea**, nun primeiro nivel, e co resto dos países noutro segundo nivel, levando a cabo macroacordos entre as entidades. A tendencia é que nun futuro inmediato haxa a obriga de que todos os prestadores no marco europeo se admitan entre eles, tendendo progresivamente cara a unha conxunción de sistemas tecnolóxicos e informáticos, logrando un marco europeo de homologación único e, probablemente, creando unha autoridade común europea ou un órgano intermediario en materia de identificación dixital que actúe de enlace entre todos os países e as súas entidades de certificación dixital.

Actualmente **estase a discutir sobre como liberar as políticas en materia de certificación dixital** xa que, aínda agora, existen certificados con políticas moi restritivas, o que provoca que nalgúns casos unha persoa deba dispoñer obrigatoriamente de varios certificados. Esta situación tamén determina a necesidade de que funcione un organismo de carácter supranacional que realice as validacións de identidade.

Hoxe en día, aínda que existen diversos proxectos para o uso da certificación electrónica a nivel europeo e internacional, estes estanse a encontrar con graves dificultades de interoperabilidade debido aos diferentes sistemas de uso dos certificados, como as certificacións cruzadas, nas que é difícil delimitar as responsabilidades entre as partes. Na actualidade aínda non se chegou a unha solución global neste aspecto.

Neste sentido, traballouse a nivel europeo no **proxecto STORK**, para conseguir o recoñecemento paneuropeo das identidades electrónicas e a nivel español na creación dunha liña TSL's, ou listas de confianza interoperables entre estados membros.

Para España, especificamente, é moi importante dende o punto de vista económico, ser interoperable con países de Latinoamérica, posto que son vías de negocio para os provedores de servizo españois.

PROVEDORES DE SERVIZOS

O mercado ao redor da certificación dixital é aínda incipiente en España a pesar de que o noso país conta xa cun número considerable de prestadores de servizos.

A situación actual do mercado en relación aos provedores de servizos parece prognosticar a posible desaparición dos pequenos provedores ou o establecemento de alianzas entre eles para xerar servizos de calidade e de valor engadido, optimizando os recursos. Todos os prestadores de servizos de certificación comparten un espazo común, no que a competencia e a competitividade son boas, e será a lei da oferta e a demanda a que decida **que provedores de servizos de certificación continuarán e cales desaparecerán**.

A longo prazo parece lóxico que unicamente se utilicen os certificados de empregado público e os certificados de atributo ou empresariais, que permitirán a supervivencia das entidades de certificación públicas e privadas e o DNIe.

En España, á creación de organismos prestadores de servizos de certificación dixital a nivel estatal, públicos e privados, uníronse tamén as iniciativas das comunidades autónomas que optaron por dispoñer de autoridades propias, diferentes e adaptadas á súa realidade

En principio, o feito de que unha Comunidade Autónoma ou mesmo unha corporación local decida converterse en entidade de certificación non parece responder a unha cuestión de aforro económico, posto que é máis rendible compartir recursos que desenvolver un servizo propio, nin de compatibilidade ou tecnolóxica.

A **creación de autoridades de certificación propias nas comunidades autónomas** está xustificada sempre e cando estas teñan unha orientación global, emitan documentos que sirvan para realizar tramitacións en calquera outra comunidade autónoma e cumpran outra serie de calidades de valor engadido Unha comunidade autónoma non debe ser só un terceiro de confianza ou un simple validador que dá crédito e fe, senón que debe ser a vangarda da administración electrónica, ofrecendo servizos de valor engadido aos cidadáns e fomentando o uso e o desenvolvemento da certificación electrónica na administración coas necesarias garantías de seguridade, confidencialidade, autenticidade e irrevogabilidade das transaccións.

LEXISLACIÓN

Xeralmente **a lexislación sobre certificación dixital foi, como noutros moitos aspectos tecnolóxicos, sempre por detrás dos avances do mercado, aínda que hoxe en día esta cuestión se estabilizou**. Na actualidade, esa lexislación que ata hai uns anos era unha das barreiras máis importantes no desenvolvemento de aspectos clave en torno á certificación

dixital deixou de ser un impedimento e converteuse nun impulso para este.

Actualmente, **a lexislación existente é suficientemente ampla** e trátase agora de, cumprindo o establecido na lei, explicarlle ao cidadán que é o que pode facer dun xeito sinxelo e claro e elaborar sistemas de información que garantan que calquera usuario poida utilizar o ámbito que desexe garantindo o principio de interoperabilidade e de neutralidade tecnolóxica. A lexislación actual supuxo a eliminación de barreiras que impoñen unha serie de retos moi importantes en materia de certificación dixital aínda que sempre respecto ás obrigas da administración.

O obxectivo é agora **conseguir, polo menos a nivel estatal, desenvolver unha normativa común** posto que un exceso de leis e regulamentacións a nivel de concellos, comunidades autónomas... podería provocar inseguridade xurídica. A lexislación actual contén aínda conceptos non demasiado claros polo que a súa aplicación, nalgúns aspectos, é diversa.

Neste aspecto destácanse como puntos clave a Lei 59/2003, do 19 de decembro, que equipara a sinatura electrónica coa sinatura manuscrita, e a Lei 11/2007, do 22 de xuño, que obriga a Administración Pública a dotarse dos medios e sistemas electrónicos que permiten aos cidadáns exercer o seu dereito a comunicarse coas Administracións por medios electrónicos e o Real Decreto 1671/2009, polo que se desenvolve parcialmente a citada Lei 11/2007 no ámbito da Administración Xeral do Estado.

Os dereitos dos cidadáns recoñecidos na Lei 11/2007, do 22 de xuño, que obriga á Administración Pública a poñer todos os servizos ofrecidos en Internet aínda non son os suficientemente coñecidos e entendidos a nivel cidadanía, aínda que xa se recoñece hoxe en día o papel pioneiro de España no recoñecemento dos dereitos do cidadán a través de Internet.

A lexislación existente actualmente pon os piares claves da xestión de identidades, do documento electrónico con garantías xurídicas, do arquivo documental,… que agora deberán evolucionar sincronizando aspectos tan diversos como o tecnolóxico, o de regulación e o de procedementos.

8. ANEXOS

8.1. Anexo I: Lexislación e normativa

8.1.1. LEXISLACIÓN AUTONÓMICA

- **Decreto 198/2010, do 2 de decembro, polo que se regula o desenvolvemento da Administración electrónica na Xunta de Galicia e nas entidades dela dependentes**

  Artigo 1º. -Obxecto.

  Este decreto ten por obxecto regular o dereito dos cidadáns a relacionarse coas administracións públicas por medios electrónicos, a tramitación dos procedementos administrativos incorporados á tramitación telemática, a creación e regulación da sede electrónica, a creación da edición electrónica do Diario Oficial de Galicia e do Rexistro Electrónico, o impulso e desenvolvemento dos servizos electrónicos e o establecemento de infraestruturas e servizos de interoperabilidade.

  REFERENCIA:

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

- **Orde de 12 de febreiro de 2010 pola que se regulan os procedementos do sistema electrónico de facturación da Xunta de Galicia**

  Artigo 1º. -Obxecto.

  Esta orde ten por obxecto desenvolver, ao abeiro do artigo 15 do Decreto 3/2010, polo que se regula a factura electrónica e a utilización de medios electrónicos, informáticos e telemáticos en materia de contratación pública da Administración da Comunidade Autónoma de Galicia e entes do sector público dela dependentes, os procedementos de tramitación de facturas no sistema electrónico de facturación coa finalidade de ofrecer un punto de referencia único aos empresarios ou profesionais que están obrigados a expedir factura polas entregas de bens e prestacións de servizos que realicen no desenvolvemento da súa actividade.

  REFERENCIA:

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

8.1.2. LEXISLACIÓN ESTATAL

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

  Artigo 1. Obxecto.

  1. Esta lei regula a sinatura electrónica, a súa eficacia xurídica e a prestación de servizos de certificación.

  2. As disposicións contidas nesta lei non alteran as normas relativas á celebración, formalización, validez e eficacia dos contratos e calquera outros actos xurídicos nin as relativas aos documentos en que uns e outros consten.

  REFERENCIA:

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

- **Lei 11/2007, de Acceso Electrónico dos Cidadáns aos Servizos Públicos**

  Artigo 1. Obxecto da Lei

  1. A presente Lei recoñece o dereito dos cidadáns a relacionarse coas Administracións Públicas por medios electrónicos e regula os aspectos básicos da utilización das tecnoloxías da información na actividade administrativa, nas relacións entre as Administracións Públicas, así como nas relacións dos cidadáns con estas coa finalidade de garantir os seus dereitos, un tratamento común ante elas e a validez e eficacia da actividade administrativa en condicións de seguridade xurídica.

  2. As Administracións Públicas utilizarán as tecnoloxías da información de acordo co disposto na presente Lei, asegurando a dispoñibilidade, o acceso, a integridade, a autenticidade, a confidencialidade e a conservación dos datos, informacións e servizos que xestionen no exercicio das súas competencias.

  REFERENCIA:

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

- **Real Decreto 1671/2009, do 6 de novembro, polo que se desenvolve parcialmente a Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos**

  Artigo 1. Obxecto e ámbito de aplicación.

  1. O presente real decreto ten por obxecto desenvolver a Lei 11/2007, do 22 de xuño,

de acceso electrónico dos cidadáns aos servizos públicos no ámbito da Administración Xeral do Estado e os organismos públicos vinculados ou dependentes desta, no relativo á transmisión de datos, sedes electrónicas e punto de acceso xeral, identificación e autenticación, rexistros electrónicos, comunicacións e notificacións e documentos electrónicos e copias.

2. As súas disposicións son de aplicación:

a) Á actividade da Administración Xeral do Estado, así como dos organismos públicos vinculados ou dependentes desta.

b) Aos cidadáns nas súas relacións coas entidades referidas no parágrafo anterior.

c) Ás relacións entre os órganos e organismos aos que se refire o parágrafo a).

REFERENCIA:

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

- **Real Decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Seguridade no ámbito da Administración Electrónica**

Artigo 1. Obxecto.

1. O presente real decreto ten por obxecto regular o Esquema Nacional de Seguridade establecido no artigo 42 da Lei 11/2007, do 22 de xuño, e determinar a política de seguridade que se ha de aplicar na utilización dos medios electrónicos aos que se refire a citada lei.

2. O Esquema Nacional de Seguridade está constituído polos principios básicos e requisitos mínimos requiridos para unha protección axeitada da información. Será aplicado polas Administracións públicas para asegurar o acceso, integridade, dispoñibilidade, autenticidade, confidencialidade, trazabilidade e conservación dos datos, informacións e servizos utilizados en medios electrónicos que xestionen no exercicio das súas competencias.

REFERENCIA:

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

- **Real Decreto 4/2010, do 8 de xaneiro, polo que se regula o Esquema Nacional de Interoperabilidade no ámbito da Administración Electrónica**

Artigo 1. Obxecto

1. O presente real decreto ten por obxecto regular o Esquema Nacional de Interoperabilidade establecido no artigo 42 da Lei 11/2007, do 22 de xuño.

2. O Esquema Nacional de Interoperabilidade comprenderá os criterios e recomendacións de seguridade, normalización e conservación da información, dos formatos e das aplicacións que deberán ser tidos en conta polas Administracións públicas para asegurar un axeitado nivel de interoperabilidade organizativa, semántica e técnica dos datos, informacións e servizos que xestionen no exercicio das súas competencias e para evitar a discriminación aos cidadáns por razón da súa elección tecnolóxica.

REFERENCIA:

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

- **Lei Orgánica 15/1999, de Protección de Datos Persoais**

Artigo 1. Obxecto

A presente Lei Orgánica ten por obxecto garantir e protexer, no que concirne ao tratamento dos datos persoais, as liberdades públicas e os dereitos fundamentais das persoas físicas, e especialmente da súa honra e intimidade persoal e familiar.

REFERENCIA:

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

- **Real Decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei Orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal**

Artigo 1. Obxecto

1. O presente regulamento ten por obxecto o desenvolvemento da Lei Orgánica 15/1999, do 13 de decembro, de Protección de datos de carácter persoal.

2. Así mesmo, o capítulo III do título IX deste regulamento desenvolve as disposicións relativas ao exercicio pola Axencia Española de Protección de Datos da potestade sancionadora, en aplicación do disposto na Lei Orgánica 15/1999, do 13 de decembro, no título VII da Lei 34/2002, de 11 de xullo, de Servizos da sociedade da información e de comercio electrónico, e no título VIII da Lei 32/2003, de 3 de novembro, Xeneral de Telecomunicacións.

REFERENCIA:

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

- LEI 56/2007, do 28 de decembro, de Medidas de Impulso da Sociedade da Información

REFERENCIA:

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

OUTRA LEXISLACIÓN E NORMATIVA NACIONAL

- Orde ITC/1475/2006, do 11 de maio, sobre utilización do procedemento electrónico para a compulsa de documentos no ámbito do Ministerio de Industria, Turismo y Comercio. (BOE 16-05-2006)
- Orde EHA/3636/2005, do 11 de novembro, pola que crea o rexistro telemático do Ministerio de Economía y Hacienda. (BOE 24-11-2005)
- Orde ITC/3928/2004, do 12 de novembro, pola que crea un rexistro telemático no Ministerio de Industria, Turismo y Comercio. (BOE 01-12-2004)
- Orde HAC/1181/2003, do 12 de maio, (BOE 15-05-2003) pola que se establecen normas específicas sobre o uso da sinatura electrónica nas relacións tributarias por medios electrónicos, informáticos e telemáticos coa Agencia Estatal de Administración Tributaria
- Resolución de 24 de xullo de 2003 da Dirección General de la Agencia Estatal de Administración Tributaria pola que se establece o procedemento a seguir para a admisión de certificados de entidades prestadoras de servizos de certificación electrónica
- Orde ECO/2579/2003, do 15 de setembro, pola que se establecen normas sobre o uso da sinatura electrónica nas relacións por medios electrónicos, informáticos e telemáticos co Ministerio de Economía e os seus Organismos adscritos.
- Orde EHA/3256/2004, do 30 de setembro, pola que se establecen os termos nos que poderán expedirse certificados electrónicos ás entidades sen personalidade xurídica a que se refire o artigo 35.4 da Lei Xeral Tributaria.

8.1.3. LEXISLACIÓN COMUNITARIA

- **Directiva 1999/93/CE del Parlamento Europeo y del Consejo, do 13 de decembro de 1999, pola que se establece un marco comunitario para a sinatura**

electrónica.

- Decisión da comisión do 14 de xullo de 2003 relativa á publicación dos números de referencia das normas que gozan de recoñecemento xeral para produtos de sinatura electrónica, de conformidade co disposto na **Directiva 1999/93/CE del Parlamento Europeo y del Consejo**.
- Directiva 2006/123/CE **del Parlamento Europeo y del Consejo**, do 12 de decembro de 2006, relativa aos servizos no mercado interior (Directiva Bolkestein).
- Norma europea "ETSI 101 456: Requisitos para a política de certificación das autoridades de certificación que emiten certificados recoñecidos".
- Directiva 95/46/CE **del Parlamento Europeo y del Consejo,** do 24 de outubro de 1995, relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos.

8.2. Anexo II: Referencias e bibliografía

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

Alberto López Tallón

Primeira Edición - Setembro 2010 (edición revisada)

ISBN: 978-84-614-3413-8

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

La factura electrónica

Manuales Plan Avanza

ISBN: 84-611-4740-5

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

Prestadores de Servizos de Certificación de Firma Electrónica (MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO):

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

8.3. Anexo III: Glosario de termos

Activación

É o procedemento polo cal se desbloquean as condicións de acceso a un crave e permítese o seu uso. No caso da tarxeta do DNIe o dato de activación é a clave persoal de acceso (PIN) e/ou os patróns das impresións dactilares (biometría).

Axencia de Protección de Datos -APD

Organismo oficial creado en España en 1993 como consecuencia da aprobación da LORTAD (Lei Orgánica de Regulación do Tratamento Automatizado dos Datos de Carácter Persoal). A súa finalidade é protexer os cidadáns contra as invasións da súa intimidade realizadas mediante medios informáticos, segundo establece o artigo 18.4 da Constitución Española.

Algoritmo criptográfico

Os algoritmos que teñen por finalidade o tratamento do segredo da información denomínanse criptográficos e son esenciais para a sinatura electrónica, xa que permiten o uso de cifras seguras para a produción e comprobación da sinatura electrónica.

API (*Application Programming Interface* - Interface de Programación de Aplicacións)

Grupo de rutinas (conformando unha *interface*) que prové un sistema operativo, unha aplicación ou unha biblioteca, que definen como invocar dende un programa un servizo que estes prestan. Noutras palabras, unha API representa un *interface* de comunicación entre compoñentes software.

O software que prové a funcionalidade descrita por unha API dise que é unha implementación do API. O API en si mesmo é abstracto, onde especifica unha interface e non dá detalles de implementación.

Arquivo con extensión ".CSR"

Son as siglas de *Certificate Signing Request*, que quere dicir "Solicitude de certificación". Un arquivo de solicitude de certificación indica cal é a clave pública a certificar e cales son os datos: nome, atributos, etc.

Arquivo con extensión ".p12" ou "pfx"

Estes ficheiros conteñen un certificado dixital, xunto coa clave privada correspondente e os certificados de todas as autoridades de certificación ata a que é a raíz (ou, como se adoita dicir, a cadea de certificación).

Autenticación

Procedemento de comprobación da identidade dun solicitante ou titular de certificados de DNIe.

Autenticidade documental electrónica

A autenticidade é unha propiedade do documento electrónico que nos informa do feito de que o documento teña unhas determinadas características.

Autoridade de certificación (AC)

Unha autoridade de certificación é un sistema informático dedicado á emisión e xestión posterior de certificados dixitais, incluíndo a renovación, expiración, suspensión, a habilitación e a revogación de certificados, a petición da autoridade de rexistro. A emisión de certificados faise dunha forma automatizada e non sen a previa confirmación da autoridade local de rexistro. Son funcións básicas das autoridades de certificación: 1) verificar a identidade dos solicitantes de certificados e 2) publicar as listas de revogación de certificados.

Autoridade de selado de data e hora

Unha autoridade de selado de data e hora (en inglés TSA, *Time Stambping Authority*) é un sistema informático dedicado ás funcións de emisión de selos de data e hora criptográficos nas condicións necesarias de calidade e seguridade, e en concreto, da xestión da fonte fiable de data e hora, que debe estar sincronizada coa hora oficial.

Autoridade de validación

É o compoñente que ten como tarefa subministrar información sobre a vixencia dos certificados electrónicos que, á súa vez, fosen rexistrados por unha Autoridade de Rexistro e certificados pola Autoridade de Certificación.

Cadea de certificados

As cadeas de certificados permiten que os empregados públicos de dúas administracións públicas se envíen documentos asinados e verifiquen correctamente as sinaturas.

Caducidade

Os certificados teñen un período de validez determinado. Unha vez este pasou, se non foi renovado, o certificado deixa de estar operativo e polo tanto, deixa de estar vixente.

Certificado de autenticación

Ten como finalidade garantir electronicamente a identidade do cidadán ao realizar unha transacción telemática. O Certificado de Autenticación (*Digital Signature*) asegura que a comunicación electrónica se realiza coa persoa que di que é. O titular poderá, a través do seu certificado, acreditar a súa identidade fronte a calquera xa que se encontra en posesión do certificado de identidade e da clave privada asociada a este.

O uso deste certificado non está habilitado en operacións que requiran non repudio de orixe, polo tanto os terceiros aceptantes e os prestadores de servizos non terán garantía do compromiso do titular do DNI co contido asinado. O seu uso principal será para xerar mensaxes de autenticación (confirmación da identidade) e de acceso seguro a sistemas informáticos (mediante establecemento de canles privadas e confidenciais cos prestadores de servizo).

Este certificado pode ser utilizado tamén como medio de identificación para a realización dun rexistro que permita a expedición de certificados recoñecidos por parte de entidades privadas, sen verse estas obrigadas a realizar un forte investimento no despregamento e mantemento dunha infraestrutura de rexistro.

Certificado dixital

Un certificado dixital é un documento electrónico asinado por unha autoridade de certificación que garante ás terceiras persoas que o reciben ou o utilizan unha serie de manifestacións nel contidas, como por exemplo, a identidade da persoa, as autorizacións, a súa capacidade para realizar un determinado acto, etc.

O certificado dixital permite ás partes ter confianza nas transaccións en Internet, polo tanto, garante a identidade do seu posuidor en Internet mediante un sistema seguro de claves administrado por unha terceira parte de confianza, a autoridade de certificación. O certificado permite realizar un conxunto de accións de forma segura e coa validez legal: asinar documentos, entrar en lugares restrinxidos, identificarse fronte a administración, etc.

Certificado recoñecido

Certificado expedido por un Prestador de Servizos de Certificación que cumpre os requisitos establecidos na Lei en canto á comprobación da identidade e demais circunstancias dos solicitantes e á fiabilidade e as garantías dos servizos de certificación que presten, de conformidade co que dispón o capítulo II do Título II da Lei 59/2003, do 19 de decembro, de Firma Electrónica.

Certificados de identidade pública

Emitidos como Certificados Recoñecidos, vinculan unha serie de datos persoais do cidadán a unhas determinadas claves, para garantir a autenticidade, integridade e non repudio. Esta información está asinada electronicamente pola Autoridade de Certificación creada ao efecto.

Cifra criptográfica

Unha cifra é un mecanismo criptográfico para protexer unha información (sexa unha comunicación en tránsito ou un documento máis ou menos perdurable) de maneira que os terceiros non autorizados non poidan acceder.

Cifrado

É o proceso que se aplica a uns datos para facelos incomprensibles e evitar que poidan ser observados por outras persoas. Este proceso ou transformación precisa dunha clave de cifrado, que é unha cadea aleatoria de bits. Só aplicando o proceso contrario, denominado descrifrado, aos datos cifrados será posible rexenerar os datos orixinais (e, polo tanto, facelos outra vez comprensibles).

Esta segunda transformación precisa dunha clave de descrifrado determinada, e que será a mesma clave de cifrado se se traballa dentro dun sistema de claves simétricas, ou doutra clave matematicamente relacionada, complementaria, da clave de cifrado, cando se traballa dentro dun sistema de claves asimétricas.

Cidadán

Toda persoa física con nacionalidade española que solicita a expedición ou renovación dun Documento Nacional de Identidade ante un funcionario da Dirección Xeral da Policía.

Clave criptográfica

As claves criptográficas son os elementos numéricos que forman unha cifra criptográfica e que funcionan conxuntamente cos algoritmos criptográficos para xerar sinaturas electrónicas e as formas de autenticación ou para facer confidencial un documento.

Clave pública

A clave pública é necesaria para comprobar a identidade do emisor ou a autenticidade dun documento asinado. Permite validar unha sinatura que fose xerada coa clave privada complementaria.

A clave pública é o único elemento do certificado dixital que se pode encontrar ao alcance de calquera. As claves públicas están dispoñibles en directorios publicados en Internet e nalgún caso en bases de datos corporativas. Relaciónase, mediante procedementos matemáticos, con outro elemento (clave privada) para garantir a súa confidencialidade e integridade. A clave pública serve basicamente para cifrar, aínda que tamén se utiliza para verificar sinaturas dixitais.

Calquera persoa pode cifrar unha mensaxe utilizando a clave pública, pero só o posuidor da clave privada pode descifralo.

Clave privada

A clave privada é o elemento secreto do certificado. Está relacionado, mediante procedementos matemáticos, con outro elemento (clave pública). A clave privada gárdase na tarxeta intelixente da persoa certificada e, polo tanto, ten todas as garantías de seguridade, aínda que se poida encontrar en repositorio ou en chave USB. Serve, basicamente, para descifrar as mensaxes recibidas, aínda que tamén se utiliza para crear a sinatura dixital.

Clave de sesión

Clave que establece para cifrar unha comunicación entre dúas entidades. A clave establécese de forma específica para cada comunicación, sesión, rematando a súa utilidade unha vez finalizada esta.

Clave persoal de acceso (PIN)

Secuencia de carácteres que permiten o acceso aos certificados.

Cloud Computing

Informática na Nube. Tipo de tecnoloxía dos servizos informáticos que permiten ter acceso a todo tipo de información e servizos dende a rede sen necesidade de ter discos duros.

A computación en nube é un concepto que incorpora o software como servizo, tal como a Web 2.0 e outros recentes, tamén coñecidos como tendencias tecnolóxicas, onde o tema en común é a confianza en Internet para satisfacer as necesidades de cómputo dos usuarios.

CP (prácticas de certificación)

As Prácticas de Certificación recollen os procedementos e requirimentos mínimos para a emisión de certificados dixitais aos cales se axustan os prestadores de servizo de certificación. Na CP especifícase tamén como se realiza o mantemento dunha infraestrutura de clave pública baseada en Certificados. En definitiva, a CP detalla e concreta o proceso completo de certificación.

Datos de creación de sinatura (clave privada)

Son datos únicos, como códigos ou claves criptográficas privadas, que o subscritor utiliza para crear a sinatura electrónica.

Datos de verificación de sinatura (clave pública)

Son os datos, como códigos ou claves criptográficas públicas, que se utilizan para verificar a sinatura electrónica.

Directorio

Repositorio de información que segue o estándar X.500 de ITU-T.

Dispositivo seguro de creación de sinatura

Instrumento que serve para aplicar os datos de creación de sinatura cumprindo cos requisitos que establece o artigo 24.3 da Lei 59/2003, do 19 de decembro, de Firma Electrónica.

Documento electrónico

Conxunto de rexistros lóxicos almacenado en soporte susceptible de ser lido por equipos electrónicos de procesamento de datos, que contén información.

Documento de seguridade

Documento esixido pola Lei Orgánica 15/99 de Protección de Datos de Carácter Persoal cuxo obxectivo é establecer as medidas de seguridade implantadas, para os efectos deste documento, pola DGP como Prestador de Servizos de Certificación, para a protección dos datos de carácter persoal contidos nos Ficheiros da actividade de certificación que conteñen datos persoais (en diante os Ficheiros).

Encargado do tratamento

A persoa física ou xurídica, autoridade pública, servizo ou calquera outro organismo que trate datos persoais por conta do responsable do tratamento dos ficheiros.

Entidade de certificación

Persoa física ou xurídica que emite certificados, de acordo coa Lei de Firma Electrónica. En ocasións trátase como un sinónimo de autoridade de certificación, que é un compoñente técnico do servizo.

Fonte de tempo fiable

Unha fonte fiable de data e hora é un sistema informático que nos informa da hora e a data reais, en tempo universal coordinado, utilizado pola emisión de selos de data e hora criptográficos. Tipicamente utilízase o subministrado polo ROA (Real Instituto e Observatorio da Armada).

Funcións *hash* ou de resumo

Unha función *hash* é unha operación matemática de resumo que se aplica a un conxunto de datos ou mensaxe. Esta operación permite obter un resumo asociado aos datos xerais e garante que non sexan posibles dúas mensaxes diferentes cun "resumo" *hash* idéntico. Grazas a esta función as comunicacións electrónicas poden realizarse máis rapidamente porque a medida dos datos é menor e pesan menos, co cal se axiliza a transmisión de datos. Sempre que se dispoña do conxunto de datos iniciais pódese obter o resumo, pero dende o resumo non se pode obter os datos iniciais.

Garantía da sinatura electrónica

A garantía da sinatura electrónica facilítaa o prestador de servizos de certificación en relación coa calidade dos algoritmos, das claves e do seu funcionamento conxunto e correcto co resto de elementos necesarios para producir sinaturas electrónicas.

Habilitación

A habilitación consiste en volver activar un certificado que foi suspendido. Esta habilitación sempre se ha de solicitar expresamente e nun prazo máximo de 120 días dende a data da suspensión.

***Hash* ou Pegada dixital**

Resultado de tamaño fixo que se obtén tras aplicar unha función *hash* a unha mensaxe e que cumpre a propiedade de estar asociado univocamente aos datos iniciais.

HSM (módulo de seguridade hardware)

É un dispositivo hardware con capacidades criptográficas que permiten xerar e almacenar de xeito seguro claves criptográficas, tipicamente os datos de creación de sinaturas (claves privadas utilizadas en PKI). Para que sexa considerado Dispositivo Seguro de Creación de Sinatura (conforme ao que establece o artigo 24 da Lei 59/2003, do 19 de decembro, de Firma Electrónica) terá que cumprir cos requisitos establecidos pola especificación técnica CEN CWA 14169 ou equivalente (segundo a Decisión da Comisión do 14 de xullo de 2003 relativa á publicación dos nomes de referencia de lles normas con recoñecemento xeral para produtos de sinatura electrónica, de conformidade co que se dispón na Directiva 1999/93/CE do Parlamento Europeo e do Consello).

Identificación

Procedemento de recoñecemento da identidade dun solicitante ou titular de certificados de DNIe.

Identificador de usuario

Conxunto de carácteres que se utilizan para a identificación unívoca dun usuario nun sistema.

Xerarquía de confianza

Conxunto de autoridades de certificación que manteñen relacións de confianza polas cales unha AC de nivel superior garante a confiabilidade dunha ou varias de nivel inferior. No caso de DNIe, a xerarquía ten dous niveis, a AC Raíz no nivel superior garante a confianza das súas AC subordinadas.

Listas de revogación de certificados (ou listas de certificados revogados)

Lista onde figuran exclusivamente as relacións de certificados revogados ou suspendidos (non os caducados).

Módulo criptográfico hardware de seguridade

Módulo hardware utilizado para realizar funcións criptográficas e almacenar claves en modo seguro.

PKI - *Public Key Infrastructure*

Expresión referente a toda a infraestrutura necesaria para poder poñer en marcha e explotar sistemas e aplicacións que utilizan técnicas de criptografía asimétrica. A criptografía asimétrica consiste en asignar dúas claves a diferentes usuarios para que nas súas comunicacións electrónicas poden descifrar a clave o outro usuario e así certificar a súa identidade.

Prestador de servizos de certificación

Persoa física ou xurídica que expide certificados electrónicos ou presta outros servizos en relación coa sinatura electrónica.

Prestador de servizos de selos de data e hora

Un prestador de servizos de certificación que emite selos de data e hora é unha persoa física ou xurídica que produce e asina en nome seu os selos de data e hora. Polo tanto, legalmente é o responsable da calidade e seguridade do selo de tempo e responde dos danos que calquera persoa poida sufrir en caso de confiar nos selos.

Proba da sinatura electrónica

A proba da sinatura electrónica é o soporte onde se encontran os datos asinados que serán admisibles como proba documental nun xuízo.

Punto de actualización do DNIe

Terminal situado nas Oficinas de Expedición que permite ao cidadán de forma guiada, sen a intervención dun funcionario, a realización de certas operacións co DNIe (comprobación de datos almacenados na tarxeta, renovación dos certificados de Identidade Pública, cambio de clave persoal de acceso - PIN -, etc.).

Renovación

A renovación consiste en solicitar un novo certificado mediante un certificado vixente pero que está a punto de caducar. Deste xeito, durante os dous meses anteriores á caducidade dun certificado pódese solicitar a renovación e isto implica que se emita un novo certificado válido.

Revogación

Anulación definitiva dun certificado dixital a petición do subscritor, ou por propia iniciativa da autoridade de certificación en caso de dúbida da seguridade das claves.A revogación é un estado irreversible. Pódese solicitar a revogación dun certificado despois dunha situación de suspensión ou por vontade das persoas autorizadas a solicitala. Do mesmo xeito, no caso dun certificado suspendido, se pasou o período de suspensión máximo, se o certificado non foi habilitado, pasa a estar definitivamente revogado. Cando a entidade de certificación revoga ou suspende un certificado, ha de facelo constar nas Listas de Certificados Revogados (CRL), para facer público este feito.Para verificar o estado dun certificado débese consultar a CRL publicada máis recentemente da entidade de certificación que emitiu o certificado no cal se desexa confiar. Estas listas son públicas e deben estar sempre dispoñibles.

Selado de tempo

Un selo de tempo ou selo de data e hora, concretamente, é un documento que nos indica a data e hora en que se produciu un acto, mediante unha fonte de tempo fiable de data e hora. O servizo de selado de tempo permite asociar un documento a unha data e hora, e deste xeito obter evidencias (técnicas e xurídicas) de que tal acto se produciu antes dun determinado momento do tempo.

Sinatura dixital

Unha sinatura dixital é unha transformación matemática dun documento, realizada mediante unha operación de cifrado asimétrico coa clave privada do asinante.

Sinatura electrónica

A sinatura electrónica é un concepto legal, neutral dende unha perspectiva tecnolóxica, que dá cobertura ao uso de calquera tecnoloxía que permita obter as mesmas funcións, con técnicas electrónicas, informáticas e telemáticas, que a firma de documentos en soporte papel.

A Lei 59/2003 de Firma Electrónica recoñece tres tipos de sinatura electrónica, en función do certificado dixital que a xera: asina electrónica ordinaria, asina electrónica avanzada e asina electrónica recoñecida, esta última equiparada á sinatura manuscrita.

Sinatura electrónica avanzada

É aquela sinatura electrónica que permite establecer a identidade persoal do subscritor respecto dos datos asinados e comprobar a integridade destes, por estar vinculada de xeito exclusivo tanto ao subscritor, coma aos datos a que se refire, e por ser creada por medios que mantén baixo o seu exclusivo control.

Sinatura electrónica recoñecida

É aquela sinatura electrónica avanzada baseada nun certificado recoñecido e xerada mediante un dispositivo seguro de creación de sinatura.

Sinatura envolvente

É unha modalidade de sinatura electrónica que inclúe o documento que se asinou, envolvéndoo. Cando o formato de sinatura é CMS (*Cryptographic Message Syntax*) ou CAdES (CMS *Advanced Digital Electronic Signature*) tradúcese como "attached"; se o formato de sinatura é XMLdSIG (XML dixital Signature) ou XAdES (XML *Advanced Digital Electronic Signature)* tradúcese "enveloping".

Sinatura envolvida (*enveloped)*

É unha sinatura XMLdSIG (XML dixital Signature) e XAdES (XML Advanced dixital Electronic Signature) tal que o elemento signature está contido, envolvido, dentro do elemento asinado. O caso máis común é cando o elemento a asinar é o nó raíz do documento.

Sinatura separada (*detached)*

Modalidade de sinatura electrónica que non inclúe o documento que se asinou. Se a sinatura é CMS ou CAdES almacénanse por separado, en ficheiros diferentes, á sinatura e o documento que se asinou. Cando é XMLdSIG ou XAdES, a sinatura fai referencia a un elemento externo, ao XML, ou ben, a posición do elemento asinado e o node asina non implica a inclusión en ningún dos dous sentidos.

Sinaturas desatendidas

As que se xeran mediante un proceso automático yi sen a intervención de ningún operador. É necesario que os datos de creación de sinatura estean almacenados nun servidor.

Solicitante

Persoa que solicita un certificado para si mesmo.

Suspensión

Invalidación temporal dun certificado dixital como consecuencia da petición do subscritor, ou por propia iniciativa da autoridade de certificación, en caso de dúbida sobre a seguridade das claves.

Terceiro Aceptante

Persoa ou entidade diferente do titular que decide aceptar e confiar nun certificado.

Titular

Cidadán para o que se expide un certificado de identidade 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