LA IDENTIDAD [ ] DIGITAL

Una visión práctica desde la normativa y su aplicación a los elementos de la Administración Electrónica

Junta de Castilla y León

red de municipios digitales de Castilla y León

“Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica”

Art. 6 de la Declaración Universal de Derechos Humanos

ÍNDICE

PRÓLOGO

Es tan importante saber quién somos, **como que lo sepan los demás**. Esta frase que en principio puede sonar algo poética, tiene mucha mayor transcendencia que la que le podemos dar en una primera lectura. En nuestra relación con los demás necesitamos disponer de una identidad que nos caracterice y determine, como queda reflejado en el **artículo 6** de la **Declaración Universal de Derechos Humanos** con el que hemos iniciado este documento. En él, se insta a los Estados a establecer los mecanismos adecuados para que esta identificación sea posible.

El trabajo diario de cualquier Administración Pública se basa en la tramitación de determinados procedimientos que vinculan a éstas con agentes de distinta naturaleza (ciudadanos, empresas u otras Administraciones Públicas). En estos procedimientos es tan importante determinar qué hay que hacer, como quién lo tiene que hacer, por lo que la problemática asociada a la identificación es uno de los principales temas a abordar por cualquier Administración Pública.

La solución parece obvia dentro de lo que conocemos como administración tradicional o administración en papel, ya que como ejemplo, en España contamos con el DNI como forma de identificación y con la firma manuscrita como método para autenticar y vincular al firmante con el documento al que acompañe.

Pero tenemos que dar un paso más allá, sobre todo ante la imparable implantación de la **Administración Electrónica**, que ha hecho necesarios la aparición de nuevas formas de identificación, vinculadas a conceptos como **firma electrónica**, **certificado electrónico**, **sello electrónico**..., junto a otros que iremos desgranando a lo largo de este documento.

Dentro de este ámbito, el **DNI electrónico** se presenta como uno de los principales protagonistas y uno de los frutos más exitosos, y la **Ley 59/2003**, **de 19 de diciembre**, **de firma electrónica** (en adelante LFE), que regula la eficacia jurídica de la firma electrónica y la prestación de servicios de certificación, como la referencia legal a este respecto.

Tampoco podemos olvidarnos de **Ley 11/2007**, **de 22 de junio**, **de acceso electrónico de los ciudadanos a los Servicios Públicos** (en adelante LAECSP), como base sobre la que se asienta el desarrollo de la nueva Administración Electrónica en España.

La **Red de Municipios Digitales de Castilla y León** (**RMD**), consciente de la transcendencia del tema, y en línea con las actuaciones que en su marco se están llevando a cabo, presenta este documento con la intención de introducir a los responsables políticos, organizativos y al personal técnico de las Entidades Locales en la problemática asociada a la identificación digital en el ámbito de la Administración Electrónica, para que cuenten con las nociones básicas que les permita traducir al mundo digital todo lo que hasta ahora se realizaba a través del papel.

Para aquellos que no estén familiarizados, la **Red de Municipios Digitales** es una iniciativa de la Consejería de Fomento de la Junta de Castilla y León, enmarcada en la Línea Estratégica "Municipios Digitales de Castilla y León" de la **Estrategia Regional para la Sociedad Digital del Conocimiento** (**ERSDI**) **2007-2013**, que pretende impulsar la prestación de **Servicios Públicos en Línea de Calidad** en el entorno local a sus ciudadanos, empresas y organizaciones utilizando las TICs. La RMD, en la que están integrados los principales Ayuntamientos y todas las Diputaciones Provinciales de la región, coordina y apoya proyectos de Administración Electrónica y Servicios Públicos Digitales en el ámbito local.

1 INTRODUCCIÓN

La verificación de la identidad de un individuo tradicionalmente ha estado vinculada a la recopilación de una serie de rasgos que nos hace únicos, como pueden ser las huellas dactilares, nuestro aspecto físico, la edad, el lugar de nacimiento,.... En el caso de España, este tipo de atributos están recogidos en nuestro **Documento Nacional de Identidad**, que a fin de cuentas asigna a todos esos atributos, que en su conjunto nos hacen únicos, un código único que nos es designado de forma exclusiva y que sirve como **forma reconocida de identificación**. Esta necesidad de identificación, y por tanto esta solución, tiene que ser trasladada al mundo digital pero con las peculiaridades que esto supone.

En el ámbito electrónico no podemos hacer uso de los rasgos físicos que hasta ahora han sido utilizados, sino que se han tenido que desarrollar una serie de herramientas e implementar unos determinados conceptos que nos sirvan para traducir nuestra identidad a este nuevo contexto, que nos permitan conseguir **nuestra identidad digital**. Pero no basta con que los ciudadanos estén identificados, ya que si nos centramos en el caso que nos ocupa, la relación entre la Administración y sus administrados, también ésta va a necesitar de los mecanismos que faciliten su identificación, de manera que quede cubierta toda la casuística de su proceder en el ámbito digital.

Lograr este doble objetivo, identificar a ciudadanos y Administraciones Públicas, no es ni mucho menos banal. De hecho, se ha convertido en uno de los principales retos a la hora de que la Administración Electrónica se convierta en una realidad. Esto es así debido a que, dejando a un lado la complejidad intrínseca del desarrollo y la aplicación de los mecanismos que facilitan esta identidad digital, ésta va a ser el pilar fundamentar sobre el que se asiente **la confianza de los ciudadanos en el uso de los nuevos Servicios Públicos Digitales** que se pongan en marcha, y por tanto del éxito de los mismos. Pero este hecho trasciende del ámbito meramente burocrático, ya que será crucial para el desarrollo y la evolución de otros sectores emergentes como el comercio electrónico o la banca electrónica.

En este contexto, las Administraciones Públicas se han posicionado como las grandes protagonistas, ya que en ellas recae la responsabilidad de crear las condiciones de confianza en el uso de medios electrónicos (art. 3 de la LAECSP). Este hecho implica que en sus manos queda el establecimiento de las medidas necesarias para la preservación de la integridad de los derechos fundamentales, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, garantizando la legalidad en la realización de sus funciones, lo que posiciona a la firma electrónica como piedra angular.

Por lo tanto, el marco de derechos y obligaciones definido en la LAECSP sitúa a las Administraciones Públicas como agentes tanto pasivos como activos en la incorporación técnica, en cuanto a la dotación de las herramientas y recursos que hagan posible la incorporación de la firma electrónica y todo lo que ello conlleva dentro de las plataformas o software del que disponga cada Entidad, así como la incorporación de estas herramientas en la realidad del personal de la Administración, de los ciudadanos y de las empresas.

Con este documento se trata de esclarecer a los responsables de las Administraciones Locales de nuestra Comunidad los conceptos que giran alrededor de la identidad digital, despejando las posibles dudas que puedan surgir, y sirviéndoles de ayuda a la hora de poner en marcha los distintos proyectos, que entorno a la Administración Electrónica, pretendan abordar.

El desarrollo del documento gira alrededor de los conceptos y preceptos que se definen primordialmente en la **Ley 59/2003**, **de 19 de diciembre**, **de firma electrónica**, **y en la Ley 11/2007**, **de 22 de junio**, **de acceso electrónico de los ciudadanos a los Servicios Públicos**. Además, estos han sido complementados con aportaciones eminentemente prácticas que facilitan y contextualizan la realidad de nuestras Administraciones Locales en cuanto a **identidad digital**.

2

2 MARCO LEGAL

Aunque la Administración Electrónica parezca un concepto nuevo que está actualmente revolucionando a los estamentos públicos, esto no es del todo cierto, y un ejemplo de ello es el tema central de este documento, la identidad digital. En este caso concreto, el interés y preocupación de las Entidades Públicas por determinar el marco normativo que regulara la identificación, dentro del nuevo entorno que estaba siendo definido por la utilización de las TICs, se remonta diez años atrás, quedando concretado en la primera ley sobre firma electrónica, ya que la LFE no es la primera ley a este respecto.

Esta primera ley, el **Real Decreto Ley 14/1999**, **de 17 de septiembre**, **sobre firma electrónica** (en adelante R.D. 14/1999), fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones Públicas. De este modo, se pretendía potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de estas nuevas herramientas, a través de un entorno que permitiera imprimir la confianza necesaria a la hora de realizar cualquier tipo de transacción electrónica en redes abiertas, como es el caso de Internet. El citado R.D. fue en ese momento la legislación más novedosa sobre esta materia en toda Europa, ya que se adelantó a la promulgación y publicación de la **Directiva 1999/93/CE del Parlamento Europeo y del Consejo**, **de 13 de diciembre de 1999**, por el que se establecía el marco comunitario para la firma electrónica.

El objeto de ambas normas es prácticamente idéntico y ambas fueron publicadas con apenas dos meses de diferencia, lo que provocó que se tuviera que llevar a cabo la elaboración de una nueva ley reguladora de firma electrónica que incluyera los cambios que la Directiva introducía, y que constituyó la actual **Ley 59/2003**, **de 19 de diciembre**, **de firma electrónica**. Esta Ley sirvió además para actualizar el marco establecido en el R.D. 14/1999, mediante la incorporación de las modificaciones que aconsejaba la experiencia acumulada desde su entrada en vigor tanto en nuestro país como en el ámbito internacional.

Es en esta misma Ley (art. 15.1) donde se establece el concepto de **DNI electrónico o DNIe** como *"el Documento Nacional de Identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos"*, concepto que es desarrollado en el **Real Decreto 1553/2005 de 23 de diciembre**, **por el que se regula el Documento Nacional de Identidad y sus certificados de firma electrónica** (en adelante R.D. 1553/2005), lo que sitúa a este Real Decreto y a LFE como el marco normativo de referencia sobre identidad digital.

Pero el desarrollo normativo sobre firma electrónica no ha parado aquí, ya que ha sufrido modificaciones como las introducidas por la **Ley 56/2007**, **de 28 de diciembre**, **de Medidas de Impulso de la Sociedad de la Información** (en adelante LMISI), con las que se pretendía clarificar las reglas de valoración de la firma electrónica en un juicio y flexibilizar la obligación de los prestadores de servicios de certificación a la hora de comprobar los datos inscritos en registros públicos, a fin de eliminar cargas excesivas.

Dentro del marco legal que pretendemos definir, no nos podemos olvidar de la **LAECSP**, que determina entre otras cosas, el contexto de agentes y servicios que conforman el nuevo modelo de Administración al que se pretende llegar, y que como podemos deducir, y en materia de identidad digital, se asienta sobre la LFE y el R.D. 1553/2005 por el que se regula el DNIe. De forma más concreta, en su art. 13, aparece expresamente la LFE como el referente normativo en cuanto a la identificación y autenticación de los distintos agentes que intervienen (ciudadanos, empresas, empleados públicos y Administración Pública) en todo procedimiento en el que se haga uso de la Administración Electrónica, y los sistemas de firma electrónica incorporados en el DNIe como los admisibles en todo los casos para las personas físicas.

A partir de LAECSP, desde la Administración General del Estado (AGE) se han estado desarrollando una serie de normas, modelos de referencia y soluciones para facilitar el desarrollo del modelo de Administración Electrónica. Para ello, **el Consejo Superior de Administración Electrónica** ha constituido una serie de grupos de trabajo interministeriales, buscando el consenso y la eficiencia en la aplicación de la Ley. En concreto, y debido al tema que nos ocupa, tenemos que destacar el trabajo realizado por el **Grupo de identificación y autenticación**, que ha sido el encargado de desarrollar el **Esquema de identificación y firma electrónica de las Administraciones Públicas**. Este esquema constituye el marco de referencia para proveer e impulsar medidas, sistemas y regulación sobre identificación y autenticación en el seno de la Administraciones Públicas, a partir de los sistemas de identificación y autenticación recogidos en la LAECSP, y conforme al art. 4 de la LFE, en cuanto a las condiciones adicionales derivadas de la aplicación de la firma electrónica en este ámbito.

Respecto a su contenido, el esquema está conformado por tres bloques documentales definidos en función del ámbito que tratan:

- **Regulación de la Infraestructura de Clave Pública** (PKI, Public Key Infrastruture): está destinado principalmente a **los prestadores de servicios de certificación**, y establece una serie de requisitos y recomendaciones para la gestión del ciclo de vida de los nuevos certificados derivados de la LAECSP.

- **Modelo de gestión de PKI**: está dirigido a los **organismos de la Administración** y describe el modelo de gestión de confianza de la PKI.

- **Condiciones generales**: se centra en la regulación de las condiciones generales y normativas de uso de los certificados, y por tanto determina un **marco general de admisión de certificados digitales**.

Por tanto, podemos deducir que este esquema incide en la idea de definir un entorno interoperable, de ahí que forme parte de las bases del **Esquema Nacional de Interoperabilidad** (**ENI**) **y del de Seguridad** (**ENS**) constituidos a partir del desarrollo del art. 42 de la LAECSP.

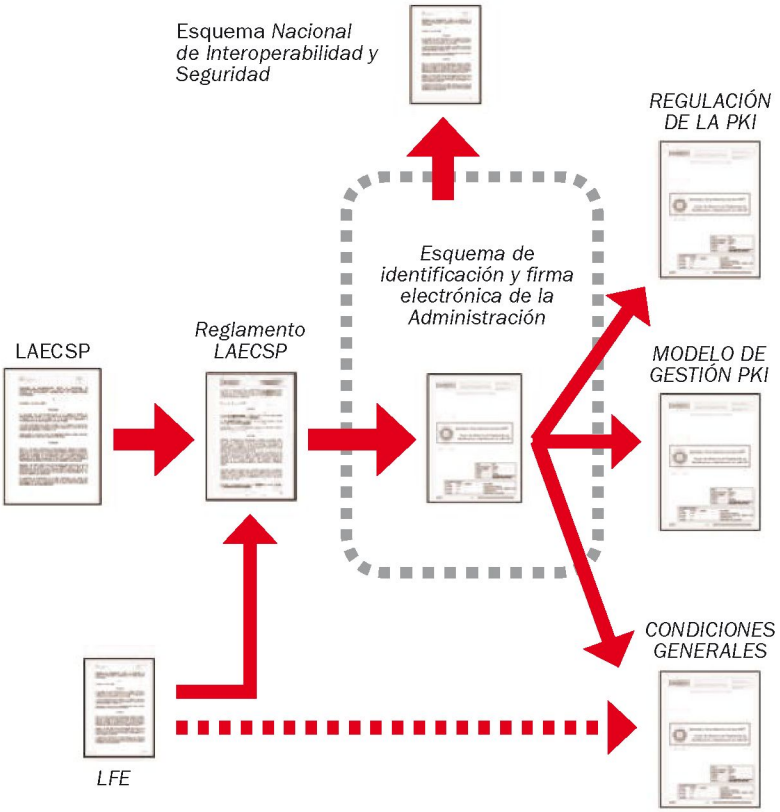


Fig.1

Esquema normativo entorno al Esquema de identificación y firma electrónica de las Administraciones Públicas[1]

1. Extraído de la definición del Esquema del identificación y firma electrónica de las Administraciones Públicas.

El ENI, en el que se determinan los criterios comunes de gestión de la información que permitan compartir soluciones y datos, y el ENS, que establece los criterios y niveles de seguridad para los procesos de tratamiento de la información, han sido **aprobados por el Consejo de Ministros el 8 de enero de 2010** y publicados en el **BOE el 29 de enero** para su entrada en vigor. Antes incluso de su aprobación, y como muestra de su papel indispensable, aparecen como herramientas básicas en el **Real Decreto 1671/2009**, **de 6 de noviembre**, **por el que se desarrolla parcialmente la LAECSP** (en adelante R.D. 1671/2009) publicado el 18 de noviembre de 2009, en el ámbito de la AGE.

Este R.D. es una referencia para el ámbito local, a la hora de establecer las pautas para que cada Administración de cumplimiento a la LAECSP.

Debido al tema que centra este documento, conocer las peculiaridades de este complejo marco normativo que se ha expuesto es fundamental, y por ello gran parte de este estudio se deriva del análisis, interpretación y aplicación de estas leyes.

3

3 CONCEPTOS BÁSICOS

3.1 FIRMA ELECTRÓNICA

El concepto de **firma electrónica** queda definido en el **art. 3 de la LFE**, como *"el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante"*. Es decir, que de realizar un garabato más o menos legible sobre un papel, identificándonos gracias a la presentación de un documento que certifica nuestra identidad, como es el DNI, y su comprobación in situ por el personal competente, vamos a pasar a adjuntar una serie de datos electrónicos, que no dejan de ser 0s y 1s, de manera automática y **más segura**. Esta reflexión permite hacernos una idea de la complejidad y el salto cualitativo que supone la incorporación de los sistemas y dispositivos que van a permitir la identificación en el entorno de la Administración Electrónica.

Otros conceptos legales que aparecen definidos también en el art. 3 de esa misma Ley, y que permiten clasificar las firmas electrónicas, son:

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

- *"Se considera **firma electrónica reconocida** la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma."*
  *"La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica **el mismo valor que la firma manuscrita en relación con los consignados en papel***", y por lo tanto, tendrá las mismas implicaciones jurídicas, lo que la sitúa como una de las protagonistas de la Administración Electrónica.

Es sobre estos conceptos, y su aplicación en el marco de la Administración Electrónica, en los que se centra el desarrollo de este documento.

Un aspecto que debemos destacar en este contexto, es la validez de la firma electrónica avanzada respecto a la reconocida. Para ello podemos remitirnos a un posible caso real, como por ejemplo encontrarnos ante un juicio en el que aportamos documentos firmados electrónicamente. Si para esas firmas se ha utilizado firma electrónica reconocida, debido a que ésta es prueba plena en un juicio, el ciudadano no tiene que demostrar su validez. Si por el contrario, se tratara de una firma electrónica avanzada, nos tendríamos que remitir a lo establecido en el apartado 2 del art. 326 de la Ley de enjuiciamiento civil, en el que se indica que sería necesario pasar por un proceso de valoración, que requeriría de un peritaje.

Tampoco podemos dejar en el aire los conceptos que caracterizan a la firma electrónica reconocida respecto a la firma electrónica avanzada, como son el **certificado electrónico reconocido**, entendido éste como el certificado electrónico expedido por un prestador de servicios de certificación que cumpla los requisitos establecidos en la LFE, del que se hablará más exhaustivamente en un apartado posterior, o el **dispositivo seguro de creación de firma** (**DSCF**), que se procede a tratar a continuación.

La LFE, en su art. 24, define un dispositivo de creación de firma como *"un programa o sistema informático que sirve para aplicar los datos de creación de firma"*. Además, en ese mismo artículo, se determinan que para que sea considerado seguro tiene que garantizar:

a) Que los datos utilizados para la generación de firma (conocidos también como **clave privada**) puedan producirse sólo una vez y que asegure razonablemente su secreto.

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

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

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

En la **Directiva 1999/93/CE** del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, en la que se establecía el marco comunitario para la firma electrónica, se hace referencia a los requisitos de los DSCF para garantizar la funcionalidad de las firmas electrónicas avanzadas, en la misma línea de los determinados en la LFE ya comentados, ya que la LFE se basa en esta Directiva.

Por otro lado, el art. 27 de la LFE viene a decir que es necesario pasar una certificación para que un dispositivo de creación de firma se considere DSCF, y que las normas técnicas de referencia aparecerían en el diario oficial de la Unión Europea.

A este respecto, en la Decisión de la Comisión Europea de 14 de julio de 2003, que viene a complementar la **Directiva 1999/93/CE** del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999 ya comentada, aparece la lista de normas que gozan de reconocimiento general para productos de firma electrónica. En esa lista, se determina que para que un sistema pueda caracterizarse como DSCF tiene que cumplir con la norma técnica **CWA 14169** (**marzo de 2002**): **secure signature-creation devices**.

En principio, los DSCF pueden ser tanto de carácter hardware como software, aunque si nos detenemos en qué dispositivos se encuentran actualmente certificados,

2. www.oc.ccn.cni.es/certificacion_es.html

mediante la información que facilita el **Organismo de Certificación** (**OC**) **del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información** (**ENECSTI**)[2], nos daremos cuenta que actualmente están certificados únicamente DSCF de carácter hardware. Por tanto, si nos centramos en este tipo de dispositivos nos vamos a encontrar:

- **Smart Cards** o tarjetas inteligentes: son aquellas que incorporan un chip que las permite tener capacidad de proceso, en el que se incorporan los mecanismos criptográficos necesarios. Este tipo de tarjetas son las utilizadas para soportar el DNIe. Para su uso es necesario disponer, además del software adecuado, un lector de este tipo de tarjetas.

- **HSM** (**Hardware Security Module**): es un DSCF que consiste en un hardware criptográfico diseñado para generar, almacenar y utilizar claves tanto simétricas como asimétricas y que aporta velocidad a las operaciones criptográficas. Cuando se opta por este tipo de dispositivo, en su memoria se almacenan las claves, y las aplicaciones que las requieran se las solicitan a él, de manera que la clave y la aplicación nunca estén en la misma máquina. Son sistemas diseñados para proporcionar un nivel alto de seguridad, ya que las firmas y las claves quedan totalmente protegidas por el hardware criptográfico en el cual fueron creadas.

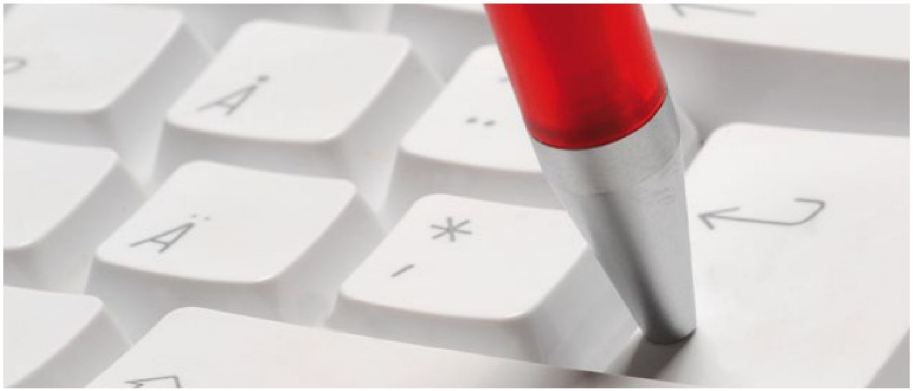
Otro aspecto que es necesario comentar es el habitual uso que se está haciendo del término **firma digital** como sinónimo de la firma electrónica, ya que no por el hecho de ser frecuente es el adecuado. Mientras que el concepto de firma digital hace referencia a una serie de métodos criptográficos, la firma electrónica es un término más amplio de naturaleza fundamentalmente legal. Un ejemplo claro de la importancia de esta distinción es el uso que de ella hizo la Comisión Europea en el desarrollo de la Directiva Europea 1999/93/CE, en la que se establece un marco europeo común para la firma electrónica. En su primer borrador se comenzó utilizando el término de firma digital, pero finalmente se acabó utilizando el término de firma electrónica para desacoplar la regulación legal de este tipo de firma y la tecnología utilizada en su implementación. Por tanto, el siguiente punto que consecuentemente hay que tratar es el de firma digital, como base técnica sobre la que se sustenta la firma electrónica.

3.2 FIRMA DIGITAL

Una vez definido este marco de conceptos teóricos, la siguiente cuestión que se nos plantea es conocer los fundamentos técnicos de la firma digital, que nos permitirá construir como abstracción a la firma electrónica.

Las Administraciones Públicas utilizan cada vez más Internet como canal para comunicarse tanto con el ciudadano como con otras Administraciones o Entidades, o incluso como canal para llevar a cabo el trabajo diario que se desarrolla en su seno. Este medio, que a priori aporta múltiples ventajas: flexibilidad en el acceso a contenidos, aumento del rendimiento debido a la reducción de tiempo, dinero y recursos que implica el uso de las Nuevas Tecnologías asociadas,..., también plantea nuevos retos a los que dar solución, de los cuales la seguridad es la piedra angular.

Nuestra máxima prioridad se va a centrar en asegurar que todo intercambio de datos se realice con las garantías de seguridad que merece según el caso, y que los ciudadanos puedan pagar un tributo, aceptar o rechazar una notificación, acceder a los datos de los procedimientos en los que estén implicados,... a través de Internet, sin que esto suponga un riesgo para ellos. Pero, ¿cómo controlar el acceso indebido a las aplicaciones y a la información almacenada?, ¿cómo garantizar la integridad o la confidencialidad de la información que viaja a través de las redes?, ¿cómo compro-



bar de manera fiable que el emisor y el receptor de una información son realmente quienes dicen ser?, o ¿cómo garantizar que el emisor no niegue haber enviado algo y el receptor no niegue haberlo recibido? Para dar respuesta a estas preguntas tenemos la **criptografía**, entendida como la ciencia que estudia los principios, métodos y medios de ocultar la información contenida en un mensaje, aunque la Real Academia Española de la Lengua facilita otra definición que la eleva a la categoría de *"Arte de escribir con clave secreta o de un modo enigmático"*.

Para poder movernos en la jerga usada en este campo, tenemos que conocer la definición de ciertos términos, lo que nos va a permitir comprender la documentación que llegue a nuestras manos sobre este tema. Entre ellos podemos destacar:

- **Texto plano o texto claro**: información original que debe protegerse.
- **Cifrado**: proceso de convertir el texto plano en un galimatías ilegible, haciendo uso de un algoritmo de cifrado.
- **Texto cifrado o criptograma**: galimatías ilegible resultado de cifrar un determinado texto plano.
- **Descifrado**: proceso inverso que recupera el texto plano a partir del criptograma y la clave.
- **Algoritmo de cifrado**: método concreto para llevar a cabo el cifrado de un texto en plano.

Para entender debidamente estos y otros conceptos se utilizarán una serie de diagramas, en los cuales se hace uso de un conjunto de símbolos, cuyo significado aparece recogido al final de este documento.

En función del objetivo que se persiga con el cifrado se usará un determinado método. Los distintos métodos existentes se fundamentan en procesos matemáticos de mayor o menor complejidad que permiten a los interesados, a partir de un código o clave, llevar a cabo el cifrado o descifrado. Podemos dividir estos métodos fundamentalmente en dos tipologías:

- **Simétricos o de clave secreta**: emisor y receptor utilizan la misma clave para cifrar y descifrar, y ésta debe permanecer en secreto entre ambos.

  El hándicap más importante que presentan es el sistema de gestión de claves ya que:

  - Es necesario contar con una forma segura de distribuir las claves, debido a que tienen que ser conocidas **sólo** por los intervinientes y en el proceso de comunicación podrían ser interceptadas, lo que sitúa a este proceso como crítico.

  - Se necesitaría trabajar con una gran cantidad de claves, ya que por cada pareja de usuarios que pretendieran establecer una comunicación segura bajo este sistema, necesitaríamos una clave. Si esto lo traducimos a números, en el caso de una red con n usuarios, para que estos se puedan comunicar se necesitarían definir $2^{n(n-1)}$ claves, lo que da una idea del volumen de claves que deberían gestionarse.

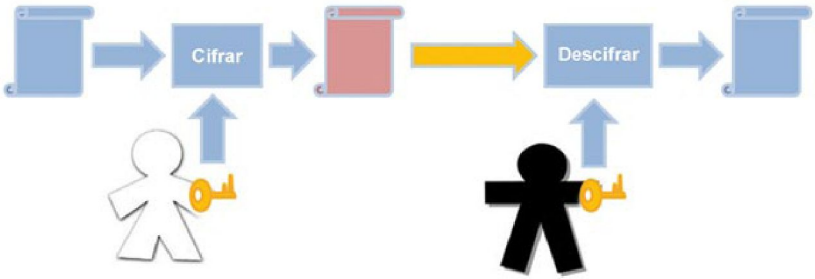


Fig.2

Encriptación simétrica

- **Asimétricos o de clave pública**: cada usuario está en disposición de un par de claves, una de carácter público (**clave pública**) y otra de carácter privado (**clave privada**). Estas claves son matemáticamente dependientes, pero de cálculo razonablemente inabordable en el tiempo estando sólo en posesión de la de carácter público. Con este algoritmo, si se cifra un texto en plano con una de las claves, éste puede ser descifrado únicamente gracias a la otra con la que forma pareja. Para comprender las aplicaciones de este algoritmo vamos a ilustrarlo con ejemplos, partiendo de la suposición de que tenemos dos usuarios implicados en la

comunicación, A y B, donde A ha generado una par de claves y ha facilitando la clave pública a B para poder comunicarse con él:

- **Encriptación con clave pública**: el usuario B cifra el documento gracias a la clave pública que le ha facilitado A, de esta manera, únicamente la persona que posea la clave privada de A va a poder descifrar el mensaje. En este caso, y debido al carácter de esta clave, solo A podrá descifrar el mensaje, de manera que solo él podrán acceder al mensaje original.

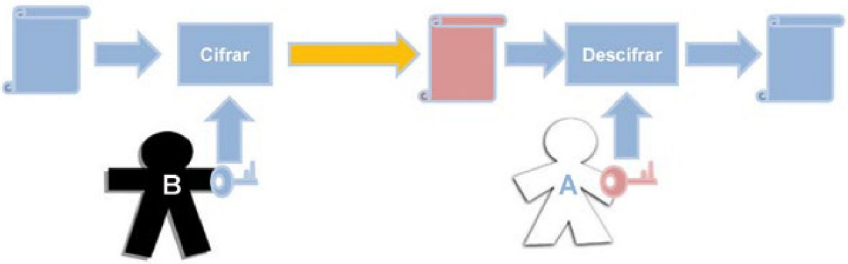


Fig.3

Encriptación asimétrica con clave pública

- **Encriptación con clave privada**: el usuario A cifra el documento gracias a su clave privada y lo envía a B. Éste descifra el documento gracias a la clave pública de la que dispone, obteniendo el documento original.

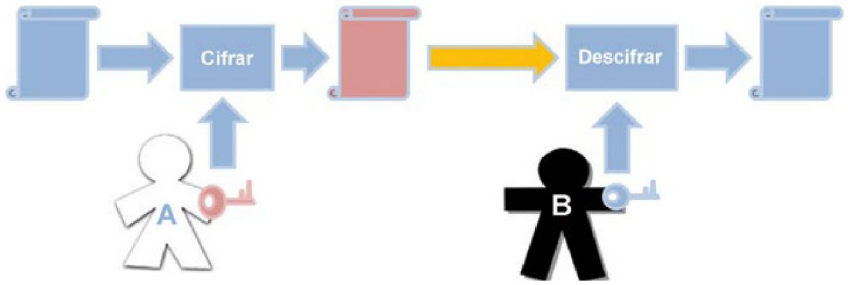


Fig.4

Encriptación asimétrica con clave privada

En este caso cualquier usuario en posesión de la clave pública de A podría descifrar el mensaje, y como es de esperar debido al carácter de ésta, tenemos que

dar por hecho que puede estar en disposición de múltiples usuarios, de manera que no tiene mucho sentido utilizar este sistema para proteger esa información de posibles curiosos, ya que no proporciona ningún tipo de confidencialidad. Pero por otro lado, sólo quien posea la clave privada que forma pareja con la clave pública utilizada por B para descifrar, puede ser el emisor del mensaje cifrado, de manera que nos puede servir para **identificar unívocamente al emisor**. Este proceso es el que se denomina **firma digital**.

El proceso de firma que se ha descrito anteriormente es lento, y con su uso únicamente podríamos identificar la autoría del documento, de ahí que en realidad, lo que se hace es trabajar con un resumen del texto en plano generado por lo que se denominan **funciones hash**, también conocidas como funciones resumen. Estas funciones se encargan de transformar un texto de longitud variable en un bloque de longitud fija en forma de resumen, y se caracterizan por ser funciones públicas e irreversibles, de manera que:

- No podemos recuperar el texto a partir del resumen.
- Es computacionalmente imposible que dos mensajes distintos tengan el mismo resumen resultado de la función hash.

El resumen obtenido de estas funciones hash, es el que se encripta con la clave privada, ya que es más rápido que tratar con el texto plano completo, y es enviado junto con el texto plano al receptor.

En este punto, ya estamos en disposición de caracterizar la firma digital, para lo que hay que destacar que:

- Sólo puede ser generada por el poseedor de la clave privada y puede ser verificada por cualquiera que conozca la clave pública del firmante.

- Es un paquete de información de tamaño fijo, dependiente del documento original, y que en la práctica se envía acompañándolo.

- Permite identificar al firmante, debido a que la clave pública con la que se desencripta sólo puede utilizarse sobre documentos encriptados con una determinada clave privada y no otra, la cual está en posesión del firmante. Este hecho permite relacionar de forma directa al documento con el firmante.

El proceso completo, desde origen hasta destino, podría concretarse de la siguiente forma:

- Cuando queramos firmar un mensaje, éste será sometido a una función hash y el resumen resultante es encriptado con la clave privada. Este resumen encriptado es enviado junto con el documento original al destinatario, ya que la prioridad no es proteger el mensaje de otros ojos, sino demostrar la autoría del mismo. Este proceso aparece representado en la figura que se adjunta a continuación.

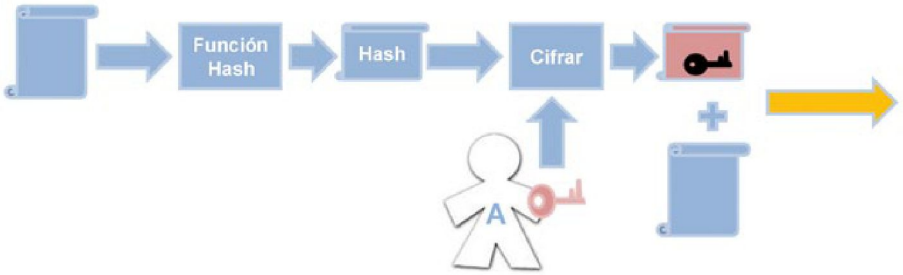


Fig.5

Proceso de firma digital en origen

- En destino, el documento original enviado sufrirá la misma función hash que en origen y, en paralelo, el resumen encriptado será desencriptado mediante la cla-

ve pública del emisor. Posteriormente se compararán los dos resúmenes hash obtenidos, con lo que así conseguiremos por un lado **verificar la autoría** (**autenticación**) del documento firmado, y por otro **comprobar que el documento no ha sufrido ningún cambio** (**integridad**) durante el envío. En la siguiente imagen se representa el proceso realizado en el destino.

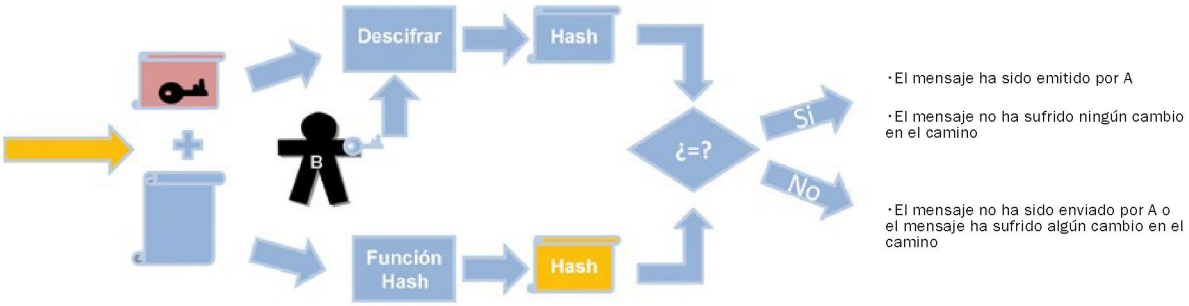


Fig.6

Proceso de firma digital en destino

A modo de conclusión, es necesario indicar que habitualmente para llevar a cabo la firma digital se hace uso de sistemas de clave asimétrica, mientras que en el caso del cifrado se suele hacer uso de sistemas de clave simétrica, ya que el cifrado con clave asimétrica supone una gran carga computacional.

3.3 CERTIFICADO DIGITAL

En el proceso descrito anteriormente se ha partido de una premisa que, aunque parezca a priori obvia, conlleva una posible fuente de problemas de seguridad, el hecho de que el emisor y el receptor están en posesión de las claves pública y privada de las que hacen uso respectivamente. Pero, ¿cómo han llegado a sus manos?, ¿cómo podemos asegurar que esas claves son de quien se dice que son?, ¿cómo podemos estar seguros de que la clave pública de un usuario, que hemos encontrado por ejemplo en un directorio o una página web, corresponde realmente a ese individuo y no ha sido falsificada por otro?

Para solucionarlo necesitamos que alguien nos de esa seguridad, **un tercero de confianza** que nos certifique la veracidad de la propiedad de la clave pública, a la que también se le conoce como **autoridad de certificación** (CA). Porque imagínate que cifras con una clave pública un documento confidencial, y esa clave pública no pertenece al destinatario al que tú pretendías enviárselo, sino a otra persona que te puede perjudicar, o la repercusión de considerar que una persona ha firmado un documento, cuando no ha sido realmente así. Si estas cuestiones de seguridad no están plenamente solucionadas acabaríamos minando la confianza de los usuarios en este tipo de sistemas, y consecuentemente, los abocaríamos al fracaso.

Para dar solución a esta problemática es necesario poder vincular la clave pública de un usuario con su identidad y para esto surge el concepto de **certificado digital**, que desde el punto de vista jurídico toma el nombre de **certificado electrónico**. Éste, en la LFE viene definido como *"el documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad"*, donde *"el firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en norme de una persona física o jurídica a la que representa"*. Además, en el art. 11 de esta misma Ley se define otro concepto, el de **certificado electrónico reconocido**, como certificado electrónico expedido por un prestador de servicios de certificación que cumpla los requisitos establecidos en la propia LFE en cuento a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten. En este mismo artículo también se indica que estos certificados electrónicos deben incluir:

"a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

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

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

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

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

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

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

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

Desde el punto de vista técnico, los certificados electrónicos admitidos tienen que estar basados en la versión 3 de la recomendación X.509 del ITU-T (International Telecommunications Union-Telecommunication), según determina el **Esquema de identificación y firma electrónica** definido por el Consejo Superior de Administración Electrónica. La estructura que presentan los certificados bajo esta recomendación queda reflejada en la siguiente imagen.

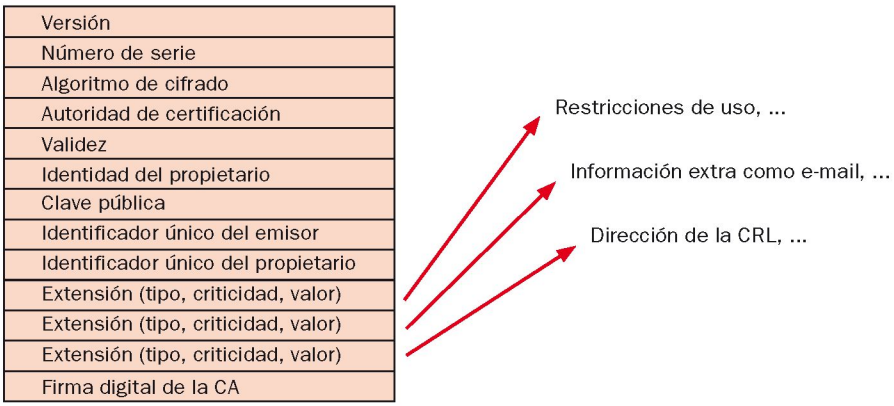


Fig.7

Esquema de la estructura del certificado electrónico X.509 v3[3]

3. La CRL es la Lista de Certificados Revocados, que contiene todos aquellos certificados que por algún motivo han dejado de ser válidos. Esta CRL debe ser actualizada y mantenida por la CA.

Por ejemplo, en el caso de tener instalado nuestro certificado personal en el ordenador y usar como navegador Internet Explorer (estaría accesible manera similar en otros navegadores), podemos acceder a la información que nuestro certificado contiene dirigiéndonos al menú *Herramientas* > *Opciones de Internet*, y una vez allí seleccionaremos la pestaña *"Contenido"*. En el apartado de certificados pulsaremos el botón de *"Certificados"* y situándonos en la ventana pulsaremos la pestaña *"Personal"*. En este apartado se muestra una pantalla con la relación de certificados personales instalados en nuestro navegador, a cuya información podemos acceder simplemente pulsando sobre ellos.

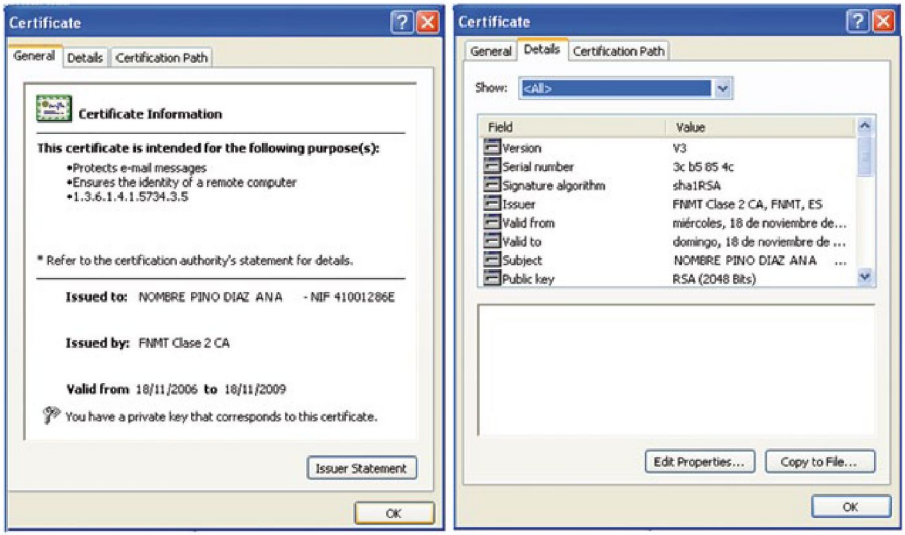


Fig.8

Ejemplo de certificado

En la imagen se muestra una composición con las capturas de pantalla correspondientes a la ventana que recoge la información general y la correspondiente a la información más detallada de un certificado concreto. En el apartado general, podemos observar que se muestra la identidad del titular del certificado, el emisor del mismo y su periodo de validez (válido desde 18/11/2006 hasta 18/11/2009). Por otra parte, se nos indica con una secuencia de números los usos y responsabilidades en relación con el certificado (1.3.6.1.4.1.5734.3.5). La correspondencia de esta

secuencia de números se encuentra en las **políticas de certificación** elaboradas por los proveedores de servicios de certificación. El ejemplo mostrado, se corresponde con un certificado emitido por la Fabrica Nacional de Moneda y Timbre (FNMT), y en su caso las políticas de certificación se encuentran incluidas en **su declaración de prácticas de certificación**[4].

La declaración de prácticas de certificación, es un documento que todo proveedor de servicios de certificación tiene obligación de formular y poner a disposición del público de forma gratuita y fácilmente accesible, al menos por vía electrónica.

En el art. 10 de la LFE, se indica que en ella se recogen *"las obligaciones que se comprometen a cumplir (los prestadores de servicios de certificación) en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros."*

Continuando con el ejemplo, si queremos más información sobre el certificado, la encontramos seleccionado la pestaña "Detalles". En ella podemos ver una clara correspondencia entre los campos que aquí aparecen y los que presenta la estructura de certificado mostrada anteriormente.

4. Se puede acceder a esta declaración de prácticas de certificación a través de la dirección: www.ceres.fnmt.es/convenio/dpc.pdf

3.4 ¿QUÉ ES UNA PKI?

Hasta ahora hemos estado definiendo y explicando conceptos criptográficos que, aunque transcendentes a la hora de entender la identificación digital, no son suficientes para reproducir por sí mismos al mundo electrónico la administración tradicional basada en papel. Para que esto sea posible necesitamos una infraestructura que nos proporcione un entorno de trabajo para un amplio conjunto de usuarios, políticas, servicios y aplicaciones, en la cual se establezcan:

- Políticas de seguridad para definir las reglas según las cuales deben funcionar.
- Productos para generar, almacenar y gestionar las claves.
- Procedimientos para establecer cómo generar, distribuir y emplear las claves y certificados.

En resumen, lo que necesitamos es una **infraestructura de clave públic**a, más comúnmente conocida como **PKI** (Public Key Infrastruture). Este tipo de infraestructuras facilitan un entorno en que los usuarios y sistemas pueden intercambiar información de forma segura, y con ellas se abarca toda la infraestructura necesaria, desde el hardware y los sistemas informáticos, hasta el material legal asociado (contratos, seguros, etc.), pasando por toda la definición de procedimientos, ciclos de vida y workflows que se utilizan. En definitiva, las PKIs nos van a permitir utilizar la criptografía de clave pública de forma fácil y efectiva.

Estos sistemas garantizan, mediante el uso de tecnologías de **clave pública**:

- **Confidencialidad**: mantener privada la información.
- **Integridad**: demostrar que la información no ha sido manipulada durante su transporte, almacenamiento o manipulación.
- **Autenticación**: demostrar la identidad de una persona o aplicación, bien como signatario de documentos o como garante para el acceso a servicios, evitando la suplantación.

- **No repudio**: garantizar que no se puede rebatir la propiedad de la información, para impedir por ejemplo, que una vez firmado un documento, el signatario se retracte o niegue haberlo redactado.

- **Autorización**: garantizar que los agentes implicados disponen de los permisos o perfiles necesarios.

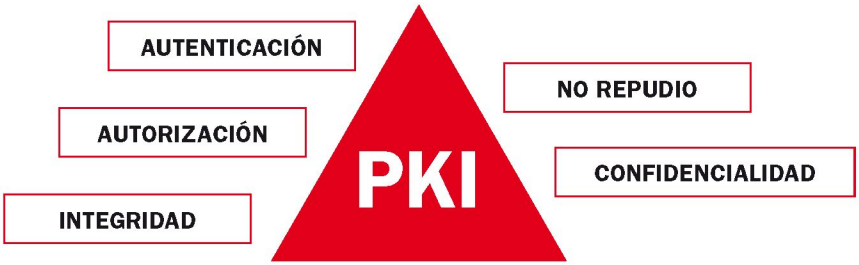


Fig.9

Garantías de una PKI

Esta PKI debe constar al menos de los siguientes elementos:

- **Autoridad de Registro** (**RA**, ***Registration Authority)***: es la entidad responsable de gestionar las solicitudes de emisión de los certificados, y por tanto, es el enlace y la responsable de verificar la relación entre la clave pública y la identidad del titular. Para ello se requiere de la presencia física del solicitante en la Autoridad de Registro, donde a través de la documentación pertinente, se verifica que el solicitante del certificado y la persona presentada son la misma persona y que la información facilitada es veraz.

- **Autoridad de Certificación** (**CA**, ***Certificate Authority)***: Es la entidad que emite los certificados, previo visto bueno de la Autoridad de Registro. Además es la encargada de proporcionar las herramientas y servicios necesarios para gestionar el ciclo de vida de los certificados que emite (emisión, suspensión y revocación). Es el tercero de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

- **Los repositorios**: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En este último, se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos.

En cuanto a los agentes que van a interactuar en este contexto, se encuentran:

- **Los Prestadores de Servicios de Certificación** (PSCs), como entidades que despliegan y mantienen estos entornos de confianza en ámbitos bien definidos, de manera que:
  - Ponen a disposición de sus usuarios herramientas para solicitar la obtención de certificados digitales de forma telemática.
  - Gestionan el ciclo de vida de los certificados electrónicos emitidos.
  - Ofrecen servicios de consulta a cerca del estado de los certificados que emiten.
  - Pueden poseer infraestructuras de Autoridad de Registro (RA), o delegar este servicio.
  - Definen jerarquías de certificación que permiten dar servicio a sus usuarios.
  - Definen sus políticas de funcionamiento.
  - Definen y ponen a disposición del público su declaración de prácticas de certificación (DPC).
- **Los usuarios y entidades finales**, que son los que utilizan las aplicaciones que hacen uso de la tecnología PKI, y para ello poseen un par de claves (pública y privada) y un certificado asociado a su clave pública.

En la siguiente figura se puede observar el funcionamiento de una PKI.

Fig.10

Infraestructura de una PKI[5]

Hay Administraciones Públicas que han optado por desarrollar su propia PKI, estableciéndose como PSCs, como es el caso del Gobierno Vasco, a través de Izenpe S.A. o de la Generalitat de Cataluña, a través de la Agència Catalana de Certificació (Catcert). En el resto de casos, a los que podemos calificar como la práctica habitual, teniendo en cuenta que este documento está dirigido a las Administraciones Locales, se contrata este tipo de servicios a PSCs ajenos a la Entidad, como por ejemplo FMNT, ACCV, Camerfirma, etc.

3.5 PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN RECONOCIDOS

Para dar a conocer los proveedores que pueden prestar servicios de certificación reconocidos, el Ministerio de Industria, Turismo y Comercio (MITYC) dispone de un buscador accesible desde la dirección **www11.mityc.es/prestadores/busquedaPrestadores.jsp**.

5. Fuente: Curso de doctorado "Seguridad en Redes de Ordenadores" de José María Sierra www.iit.upcomillas.es/palacios/seguridad_dr/tema5_pki.pdf

Este buscador, además de facilitar una relación de proveedores de servicios de certificación, aporta de cada prestador los datos de identificación, información comercial e información sobre los servicios que presta. En la figura que se adjunta a continuación se muestra el tipo de fichas que utiliza por cada prestador de servicios de certificación.

CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)

Identificación

Nombre o Razón Social:	Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)		
CIF:	Q2826004J	**Teléfono:**	-
Domicilio Social:	Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda. Departamento CERES. C/ Jorge Juan, 106, Madrid (Madrid) - 28009		
Orden de creación:	Las competencias de la FNMT-RCM quedan definidas por el Real Decreto 1317/2001 de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1999		

Información comercial

Nombre Comercial:	CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)		
Dominio:	www.cert.fnmt.es	**Teléfono:**	915666666
e-mail:	ceres@fnmt.es		
Domicilio:	Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda. Departamento CERES. C/ Jorge Juan, 106, Madrid (Madrid) - 28009		

Servicios

✔ **Servicios de certificación basados en certificados reconocidos**

Nombre
Servicios de Certificación de la FNMT-RCM. El nombre distintivo de la Autoridad de Certificación de la FNMT-RCM es: ou=FNMT Clase 2 CA, o=FNMT, c=ES

✔ **Servicios de certificación basados en certificados no reconocidos**

Nombre
Servicios de Certificación de Certificados de Persona Jurídica y de Entidades sin personalidad jurídica para el ámbito tributario. El nombre distintivo de la Autoridad de Certificación de la FNMT-RCM es: ou=FNMT Clase 2 CA, o=FNMT, c=ES

✔ **Otros servicios en relación con la firma electrónica - Servicios de validación temporal**

Nombre
Servicio de Timestamping de la FNMT-RCM

✔ **Otros servicios en relación con la firma electrónica - Servicios de custodia**

Nombre
Servicio de Custodia de Documentos Electrónicos de la FNMT-RCM

✔ **Otros servicios en relación con la firma electrónica - Otros servicios**

Nombre
Servicio de expedición de Certificados de Atributos de la FNMT-RCM

Fig.11

Ejemplo de ficha sobre proveedores de servicios de certificación emitida por el MITYC

3.6 SELLOS Y MARCAS DE TIEMPO

Este documento se centra en las necesidades de identificación y autenticación que van a tener que ser cubiertas para poder implementar una Administración Electrónica con todas las garantías. Pero para que estas necesidades sean plenamente satisfechas, se requiere poder establecer una referencia temporal con la que poder determinar el momento en el que se ha producido un determinado acto administrativo en su forma electrónica. Este requerimiento, además de ser producto del paso del mundo en papel al digital, se deriva de la propia LAECSP, ya que en varios artículos se hace mención directa o indirecta su implementación.

De forma más explícita, y dentro del art. 47 de R.D. 1671/2009, se determina lo que se denomina como **la referencia temporal de los documentos administrativos electrónicos**, contemplando las siguientes modalidades:

- *"«**Marca de tiempo**» entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo."*

- *"«**Sello de tiempo**», entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento."*

La distinción se ha hecho para evitar el uso del sello de tiempo de forma injustificada. De hecho, en la mayoría de los casos sólo es necesaria la marca de tiempo, que puede provenir de un servidor sincronizado a través de una conexión **NTP** (Network Time Protocol) con el **Real Instituto y Observatorio de la Armada** (ROA), que según R.D. 23 octubre 1992, núm. 1308/1992 y en el art. 15 del ENI, es el encargado de proporcionar **la base de la hora legal en todo el territorio nacional**. Un ejemplo de uso de estas marcas de tiempo lo encontraríamos en el intercambio de información entre administraciones, ya que para incluir la fecha y hora no es necesario contar con que éstas estén certificadas por un tercero.

Por su parte, **el sello de tiempo** será de uso necesario en servicios donde los atributos temporales sean críticos, o aquellos en los que un juez pueda requerir este dato y en los que la acreditación del propio organismo no sea suficiente, de ahí que sea necesaria la intervención de un tercero de confianza o autoridad de sellado de tiempo (TSA – Time Stamping Authority). En este grupo de servicios encontraríamos por ejemplo la obtención automatizada de imágenes electrónicas de documentos privados (art. 30 de la LAECSP).

Para conocer información más específica relativa a las características de estas marcas y sellos de tiempo asociadas a los documentos electrónicos, según la disposición adicional primera del ENI, tenemos que dirigirnos a la normativa técnica adicional dedicada a este respecto.

El esquema que se muestra a continuación, con el que se pretende clarificar el funcionamiento del proceso de sellado de tiempo entre una Administración Local y una TSA, muestra de forma detallada sus fases e intervinientes.

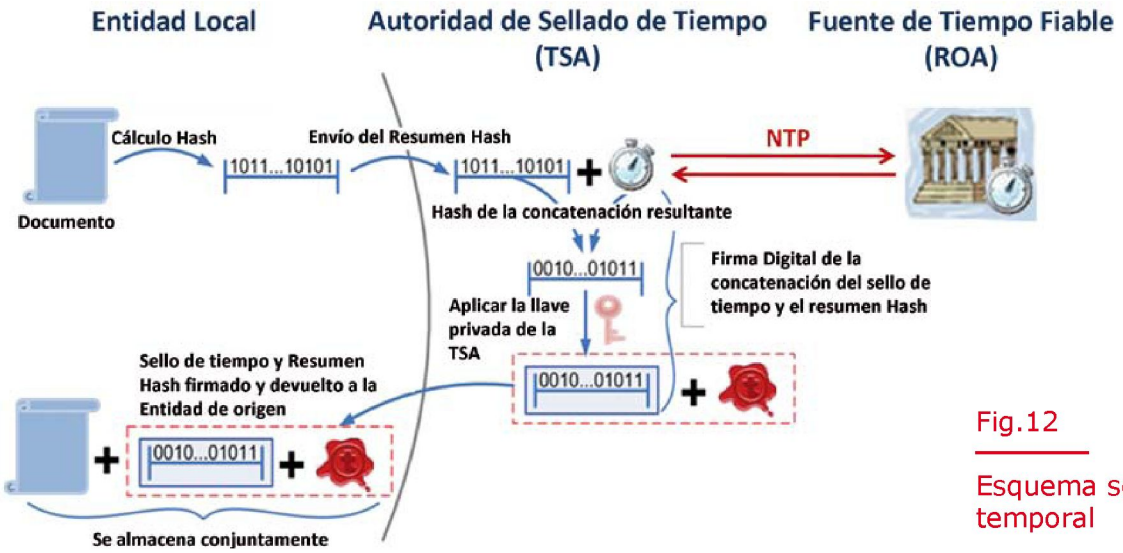


Fig.12

Esquema sobre el sellado temporal

Este modo de proceder puede resumirse como sigue:

- La Entidad Local solicitará a la TSA el sello de tiempo mediante el envío de un resumen (hash) de la información a sellar.

- Una vez recibida la solicitud, la TSA genera el sello de tiempo, con la fecha y hora obtenidas de una fuente fiable, y lo adjunta al resumen. Posteriormente, estos datos son firmados electrónicamente haciendo uso de su **clave privada**, y remitidos a la Entidad solicitante.

  Para obtener la fecha y la hora del sello de tiempo es necesario que la TSA se comunique, haciendo uso de una conexión **NTP**, con una **fuente de tiempo fiable**, en este caso el **ROA** que como ya se ha comentado es el organismo que ofrece el tiempo oficial en España.

- Por su parte, la Entidad solicitante, adjuntará ese sello de tiempo a la información de partida, lo que le proporcionará la garantía sobre la integridad de la misma en el tiempo.

- Por otro lado, la TSA debe almacenar el sello emitido para futuras verificaciones.

Además, es necesario disponer de **un servicio de cotejo de estos sellos en la sede electrónica** de la Entidad Local, para que el ciudadano pueda comprobar su validez de forma sencilla.

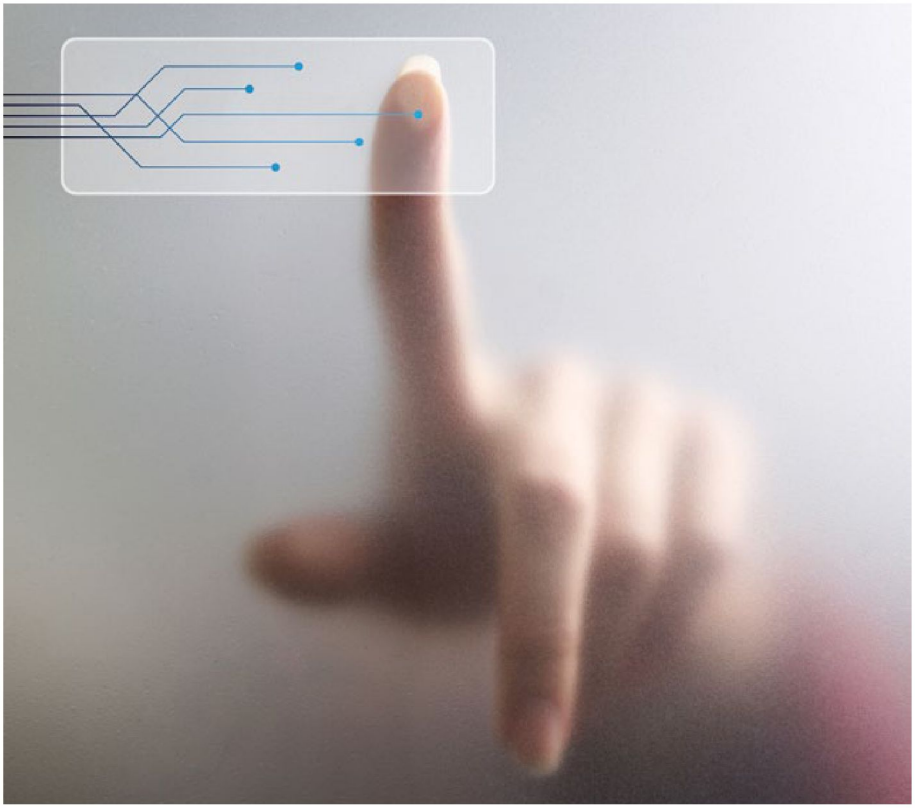
En este caso no podemos aplicar la caracterización de sellos de tiempo reconocidos o no reconocidos, ya que no existe ninguna certificación que avale este hecho, como ocurría en el caso de los certificados electrónicos antes comentados. Lo máximo que podemos llegar a considerar es el hecho de estar registrados o no por parte del MITYC. Por lo tanto nos encontraríamos con:

- Sellos de tiempo emitidos por TSA de ACs registradas por el MITYC, accesibles junto con el resto de prestadores de servicios de certificación reconocidos a través de la página web ya comentada[6].

6. www11.mityc.es/prestadores/busquedaPrestadores.jsp

- Sellos de tiempo emitidos por TSA de ACs no registradas por el Ministerio. Entre este tipo de TSA nos encontraríamos las TSA propias de una Administración (PKI propia de la Administración) o las TSA privadas (p.ej. VeriSign).

En cuanto a los efectos jurídicos de los sellos emitidos por un tipo u otro de autoridad, aunque no se ha normado todavía su peso legal, es de suponer que los sellos de tiempo emitidos por TSAs registradas por el MITYC tendrán mayores garantías jurídicas, al estar basado en una firma electrónica reconocida.



4

4 ¿QUIÉN O QUÉ NECESITA IDENTIFICACIÓN?

En el apartado anterior se han ido desgranando las bases técnicas sobre las que se asienta la firma electrónica, y por ello ya estamos en condiciones de ir definiendo y tratando los distintos conceptos de interés que rodean a la firma electrónica dentro del contexto que caracteriza el día a día de las Administraciones Públicas.

La LAECSP recoge los elementos que son necesarios para configurar un sistema de Administración Electrónica que permita poner a disposición de los ciudadanos Servicios Públicos de calidad, con las garantías que en cada caso sean exigibles, y teniendo como referencia la LFE. Durante este apartado se van a ir identificando estos elementos y determinando las necesidades que en cuanto a identificación va a ser necesario destacar.

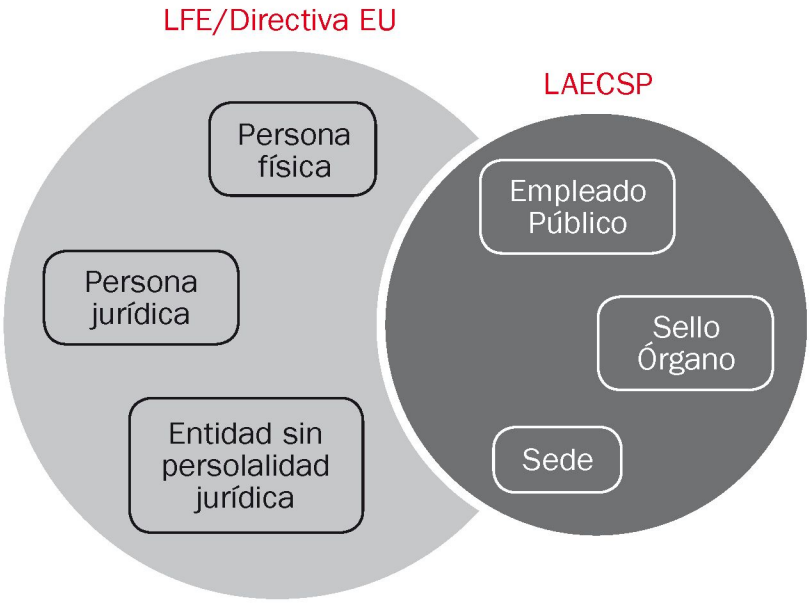


Fig.13

Marco de certificados electrónicos definidos según la LFE y LAECSP

7. Imagen extraída del documento *"Conclusiones del grupo de trabajo sobre sistemas de identificación y autenticación"*, elaborado por el Grupo de trabajo sobre sistemas de identificación y autenticación del Consejo Superior de Administración Electrónica.

Además de estas dos leyes, no nos podemos olvidar del Esquema de identificación y firma electrónica, como uno de los pilares del ENI, en el que se describe el marco de referencia general de identificación y autenticación electrónica dentro del entorno de las Administraciones Públicas. En él se definen los medios para la implantación de los nuevos sistemas de identificación y autenticación recogidos por la LAECSP, lo que permite conformar un escenario de interoperabilidad de firma electrónica en el ámbito de las Administraciones Públicas.

Tampoco podemos olvidarnos del propio ENI y del ENS, así como del R.D. 1671/2009, que nos pueden ayudar a interpretar y entender las tendencias y requerimientos a este respecto.

Si se analiza la actividad de las Entidades Públicas, se puede dividir en dos grandes grupos las necesidades derivadas de la identificación, como queda recogido a continuación.

IDENTIFICACIÓN DE LA ADMINISTRACIÓN PÚBLICA

En este punto las necesidades identificativas giran en torno a:

- La identificación de la **sede electrónica**, para lo cual se hará uso de **certificados de dispositivo seguro o medio equivalente** (art. 17 LAECSP).

- La identificación para dar soporte a **la actuación administrativa automatizada**. Para ello se hará uso del **sello electrónico**, también conocido como **sello de órgano** y basado en **certificados electrónicos**, o de los **códigos seguros de verificación** (art. 18 LAECSP).

- La identificación del **personal al servicio de las administraciones públicas**, a través **de sistemas de firma electrónica de personal** facilitados por la propia Administración, o haciendo uso de los que se incorporan en el **DNIe** personal de cada funcionario (art. 19 LAECSP).

- Identificación de las Administraciones Públicas para el **intercambio de datos** en entornos cerrados de comunicación (art. 20 LAECSP), ya sea:

- Entre miembros de la misma Entidad: será ésta la que determine las condiciones y garantías, lo que incluirá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

- Entre integrantes de distintas Administraciones: caso en el que las condiciones y garantías se determinarán a través de convenio.

Con estos sistemas de identificación y los servicios de verificación adecuados, el usuario podría confirmar, en cualquier situación de las posibles dentro de la casuística de la relación entre Administración y ciudadano, la identidad de la Entidad con la que está interactuando. Directamente, esto afianzaría la confianza depositada por el usuario en la Administración Electrónica, pilar que es esencial apuntalar para que ésta se establezca plenamente como canal.

IDENTIFICACIÓN DE LOS CIUDADANOS

Es necesario facilitar al usuario los medios para identificarse frente a la Administración, y en consecuencia, que ésta tenga la capacidad de poder determinar con qué ciudadano se está relacionando en cada momento, con las garantías suficientes, y siempre **bajo el principio de proporcionalidad**. Hay que tener en cuenta, que los datos con los que normalmente trabaja la Administración son especialmente sensibles, y que cualquier brecha de seguridad puede tener importantes repercusiones, pero con esto no hay que entender que para, por ejemplo, acceder al tablón de anuncios de la Entidad sea necesario exigir el uso del DNIe.

En este caso nos encontraríamos que la identificación gira en torno a:

- **Identificación de persona física** (art. 13 LAECSP), a través de los sistemas de firma electrónica incluidos en el DNIe, sistemas de firma electrónica avanzada, entre los que se incluye los basados en certificado electrónico reconocido, u otros que se determinen (Ej.: claves concertadas) admitidos por Entidad.

- **Identificación de persona jurídica** (art. 7 LFE), a través de certificados electrónicos de personas jurídicas. Debido a la naturaleza de este tipo de certificados, la solicitud, la custodia de los datos de creación de firma y la responsabilidad la

ostenta la persona física solicitante, y por ello, la identificación de esta persona estará incluida en el certificado electrónico. Asimismo, se pueden incluir límites adicionales de uso, definidos por la propia personalidad jurídica.

- **Identificación de una entidad sin personalidad jurídica** (Disposición adicional tercera LFE). La expedición de certificados electrónicos para la identificación de este tipo de entidades (art. 33 de la Ley General Tributaria) queda limitado al ámbito tributario.

Dentro de este grupo, no hay que olvidar las opciones de **representación** que contempla la LAECSP, entre las que encontramos:

- Identificación de ciudadanos **por funcionario público** (art. 22 LAECSP). De manera que, en el caso de que un ciudadano no esté en disposición de los instrumentos de identificación o autenticación pertinentes, un funcionario público, haciendo uso de los sistemas de firma de los que se le haya dotado, y previa identificación y consentimiento expreso del ciudadano, podrá realizar cualquier operación por medios electrónicos que éste solicite. Los funcionarios facultados para llevar a cabo estas labores aparecerán recogidos en un **registro de funcionarios habilitados** que será mantenido por cada Administración Pública.

- La identificación a través de la fórmula de **la representación a través de un tercero** (art. 23 LAECSP). Podrán habilitarse a personas físicas o jurídicas como autorizadas para la realización de determinadas transacciones electrónicas en representación de un interesado. Para ello se deben especificar las condiciones y obligaciones a las que se compromete el representante. Por su parte, la Administración podrá requerir en cualquier momento la acreditación pertinente para dicha representación.

  En este mismo sentido, en el ámbito de la AGE, el R.D. 1671/2009 prevé un régimen específico que facilita la actuación en nombre de terceros, y que puede servir de referencia para las Administraciones Locales, en el cual se establece:

  - **La posibilidad de habilitar a personas físicas o jurídicas como representantes para la presentación electrónica de documentos**. Para ello se deberá suscribir

un convenio, que incluirá, al menos, los procedimientos y trámites objeto de la habilitación, y las condiciones y obligaciones aplicables.

- **El registro electrónico de apoderamientos**, como nuevo mecanismo de acreditación, en el que se podrán hacer constar las representaciones que se otorguen a terceros en el ámbito de la AGE.

Cuando hablamos de Administración Electrónica, ésta incluye fundamentalmente el desarrollo e implantación de sistemas para el tratamiento de la información mediante el establecimiento de comunicaciones que ofrecen todas las garantías y, como se indica en el **Esquema Nacional de Seguridad**, entre otros requisitos mínimos de seguridad, se tendrá que llevar a cabo un **análisis y gestión de riesgos**. Este análisis, requerirá el estudio pormenorizado de los procedimientos y tareas llevadas a cabo por nuestro sistema, y nos permitirá conocer a fondo los requisitos que debe cumplir. De ahí que sea esencial llevar a cabo este análisis para conocer el tipo de información con la que vamos a trabajar en cada caso, el nivel de seguridad que requiere, y en consecuencia y siempre teniendo presente el **criterio de proporcionalidad**, determinar los requerimientos necesarios para la identificación de los intervienes en cada situación, así como las restricciones de acceso si procede. Lo que tenemos que intentar es adoptar la firma electrónica reconocida cuando sea necesario, pero no tender a usarla como paradigma de la identificación y autenticación.

En el transcurso de este apartado iremos comentando cada una de estas necesidades identificativas y las posibles soluciones y peculiaridades, usando para ello la misma clasificación que ha sido utilizada.

4.1 IDENTIFICACIÓN DE LA ADMINISTRACIÓN PÚBLICA

Como se ha apuntado en el apartado anterior, la identidad de las Administraciones Públicas va a ser facilitada haciendo uso de **certificados electrónicos**, pero para unificar criterios a la hora de crear estos certificados, se ha optado por seguir las directrices que a este respecto se han definido en el Esquema de identificación y firma electrónica, con la pretensión de garantizar la interoperabilidad entre las distintas Administraciones Públicas. En este esquema encontraremos los campos fijos y opcionales que aparecerán sobre la estructura de certificados basada en el **estándar X.509** ya comentada, y a los que se hará referencia durante este apartado. Estos campos determinan lo que se ha denominado como **Identidad Administrativa**, que se puede definir como un esquema de nombres incluido en los certificados, el cual facilitará la utilización de estos y la identificación del suscriptor del certificado. En la práctica esta Identidad Administrativa estará situada en un área concreta del certificado, Subject Alternative Name.

4.1.1 Sede electrónica

El concepto de sede electrónica apareció por primera vez en la LAECSP, definida en su **art. 10** como *"aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias", con la responsabilidades que ello conlleva para el titular respecto a "la integridad, veracidad y actualización de la información y servicios a los que pueda accederse".*

De forma más clara la podemos interpretar como la oficina virtual de la Entidad Pública, a la que normalmente se tendrá acceso a través de su portal web. **En ella residirán todas las actuaciones**, **procedimientos y servicios** (registro electrónico, pago electrónico, consulta del estado de sus procedimientos, consulta de los boletines oficiales,...) **que requieran de la autenticación de la Entidad Local o de los ciudadanos**, y para su diseño se *"respetarán los principios de accesibilidad y usabilidad de acuerdo con las normas establecidas al respecto, haciendo uso de estándares abiertos u otros*

que sean de uso generalizado" (art. 10.5 LAECSP). Por tanto, se tiene que desterrar la idea de que la sede electrónica es el portal web de la Entidad, y asociar este término al espacio concreto del portal web a través del cual se tiene acceso a una serie de servicios e informaciones que requieren de ciertas garantías, y de los que la Entidad se hace plenamente responsable.

En este sentido, el R.D. 1671/2009 establece incluso el conjunto de servicios característicos que deberán aparecer incluidos en las sedes electrónicas, así como el alcance de su eficacia y responsabilidad. De hecho, en el apartado 2 del art. 6 aparecen como servicios a poner a disposición de los ciudadanos los siguientes:

"a) Relación de los servicios disponibles en la sede electrónica.

b) Carta de servicios y carta de servicios electrónicos.

c) Relación de los medios electrónicos a los que se refiere el artículo 27.4 de la Ley 11/2007, de 22 de junio.

d) Enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.

e) Acceso al estado de tramitación del expediente.

f) Acceso a la publicación de los diarios o boletines.

g) Acceso a la publicación electrónica de actos y comunicaciones que deban publicarse en tablón de anuncios o edictos, indicando el carácter sustitutivo o complementario de la publicación electrónica.

h) Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.

i) Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede que hayan sido autenticados mediante código seguro de verificación.

j) Indicación de la fecha y hora oficial a los efectos previstos en el artículo 26.1 de la Ley 11/2007, de 22 de junio."

Aunque esta relación forma parte de directrices fijadas para el ámbito de la AGE, puede servir de ejemplo a las Administraciones Locales, a la hora de diseñar sus propias sedes electrónicas.

Además, y a pesar de no aparecer mencionado en este R.D., a este contenido hay que añadir, según aparece como novedad en el art. 42 de Ley 30/2007, de 30 de octubre, de Contratos del Sector Público (en adelante LCSP), la publicación del **Perfil de Contratante**.

La primera duda que como ciudadanos nos vamos a plantear a la hora de realizar un procedimiento con una Administración Pública a través de su sede electrónica es, ¿realmente estoy comunicándome con mi Administración, o este portal web al que estoy accediendo es el de un impostor? Para dar solución a esta problemática, según el art. 17 de LAECSP, *"las sedes electrónicas utilizará, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en* ***certificados de dispositivo seguro o medio equivalente***", que se materializa en el denominado **certificado de sede electrónica**.

Otro aspecto que es necesario aclarar sobre este tipo de certificados, es que su uso está limitado a la identificación de la sede electrónica, quedando **excluida su aplicación para la firma electrónica de documentos y trámites**, como queda indicado de forma explícita en el art. 18.2 del R.D. 1671/2009. Para esos casos se hará uso del certificado de sello electrónico que trataremos más adelante.

Es necesario tratar más profundamente el certificado de sede electrónica, ya que éste no puede ser definido de cualquier manera, sino que lo más adecuado es regirse por las directrices que a este respecto se han definido en el Esquema de identificación y firma electrónica, a efectos de garantizar la interoperabilidad entre las distintas Administraciones Públicas. De hecho, se definen una serie de campos fijos (en este caso no hay opcionales) que deben aparecer, y que son ratificados por el R.D. 1671/2009:

- Descripción del tipo de certificado, tomando en este caso el valor de "***sede electrónica***".
- Nombre descriptivo de la sede electrónica.
- Denominación de nombre de dominio/dirección IP.
- Nombre de la entidad suscriptora del certificado.
- Número de identificación fiscal de la entidad suscriptora.

Para ejemplarizar la cumplimentación de los campos en la estructura de un certificado, se muestra en la siguiente imagen la propuesta definida en el Esquema de identificación y firma por el grupo de trabajo constituido a tal efecto por el Consejo Superior de Administración Electrónica.

2.4. Subject Alternate Names	**Nombre alternativo de la sede electrónica**	**Si**	
2.4.3.1. Tipo de certificado	Indica la naturaleza del certificado	F	OID: 2.16.724.1.3.5.1.2.1 Tipo= "sede electrónica" (String UTF8) Size = 31
2.4.3.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.1.2.2
2.4.3.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF = NIF entidad suscriptora ej: "S2833002" (String UTF8) Size = 9 OID: 2.16.724.1.3.5.1.2.3
2.4.3.4. Nombre descriptivo de la sede electrónica	Breve descripción de la Sede indicando un nombre	F	Nombre descriptivo de la sede electrónica, asegurando que dicho nombre tenga sentido y no de lugar a ambigüedades. Nombre sede = "PORTAL 060" (String UTF8) Size = 128 OID: 2.16.724.1.3.5.1.2.4
2.4.3.5. Denominación de nombre de dominio IP	Dominio al que pertenece la Sede	F	Nombre Dominio IP = "060.es" (String UTF8) Size = 128 OID: 2.16.724.1.3.5.1.2.5

Fig.14

Extracto del perfil de certificado de sede electrónica para APE propuesto en el Esquema de identificación y firma electrónica

En la práctica, se han estado utilizando los certificados de servidores seguros con establecimiento de canal seguro (SSL - Secure Sockets Layer), para autenticar los servidores de las Administraciones Públicas que lo requieren. Sin embargo, estos certificados comúnmente empleados y aceptados por todas las partes intervinientes en

una comunicación, no están normados ni tipificados siguiendo las directrices marcadas y antes indicadas, contraviniendo al art. 42 de la LAECSP, en el que se apunta que el ENI debe ser tenido en cuenta por las Administraciones Públicas. De manera que lo deseable es que poco a poco estos certificados sean sustituidos por los descritos en este apartado, afianzando poco a poco el marco común de plena interoperabilidad que se pretende conformar.

En la siguiente imagen se muestra la sede electrónica del Consejo Superior de Deportes, y la información contenida en el campo Subject Alternative Name del certificado que actualmente utilizan. Si lo miramos detenidamente, podemos ver que en él se indica la tipología del certificado y el resto de valores antes comentados.

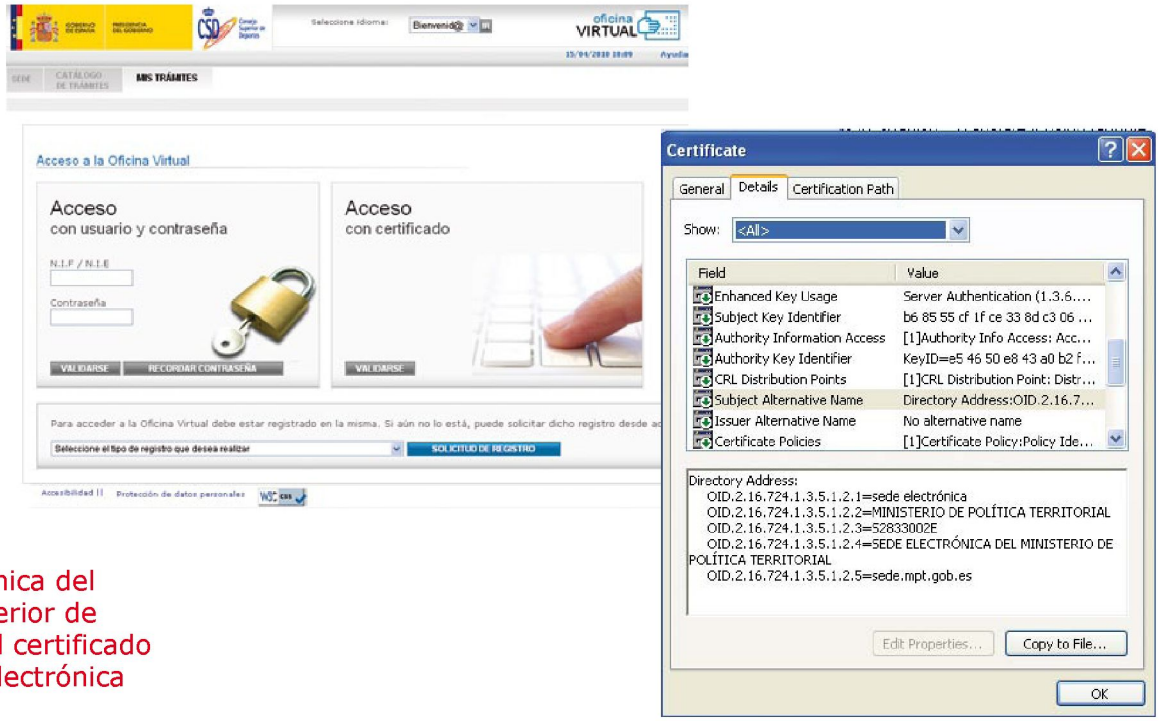


Fig.15

Sede electrónica del Consejo Superior de Deportes y el certificado de sede de electrónica que utiliza

Además, toda sede electrónica dispondrá, en cuanto a identificación se refiere, y tomando como referencia el R.D. 1671/2009 (ámbito limitado a la AGE) y la propia LAECSP, el siguiente contenido mínimo:

- La identificación del titular (art. 10.3 LAECSP y art. 3.2 R.D. 1671/2009).
- La identificación del órgano u órganos responsables de la gestión y de los servicios puestos a disposición de los ciudadanos en la misma (art. 6 R.D. 1671/2009).
- La identificación de la dirección electrónica de referencia de la sede (art. 3.2 R.D. 1671/2009).
- Un sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita (art. 6 R.D. 1671/2009).
- La relación de sistemas de firma electrónica que sean admitidos o utilizados en la sede (art. 6 R.D. 1671/2009). Dentro de esta, y como queda reflejado en el art. 15.2 de la LAECSP, estará contemplada la relación de los sistemas de firma electrónica avanzada admitidos, en la que se incluiría al menos, información sobre los elementos de identificación utilizados, así como en su caso, las características de los certificados electrónicos admitidos, los prestadores que los expiden y las especificaciones de la firma electrónica que puede realizarse con dichos certificados.
- La relación de sellos electrónicos utilizados por la Entidad, incluyendo las características de los certificados electrónicos y los prestadores que los expiden (art. 18.3 LAECSP).
- Cada Administración adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos (art. 18.3 LAECSP), lo que implica que tienen que poner a disposición de los ciudadanos sistemas que permitan esta verificación.
- Identificación de los canales de acceso a los servicios disponibles en la sede, así como en su caso, los teléfonos y oficinas a través de los cuales también puede accederse a los mismos (art. 3.2 R.D. 1671/2009).

- Cualquier otra circunstancia que se considere conveniente para la correcta identificación de la sede y su fiabilidad (art. 3.2 R.D. 1671/2009).

Uno de los aspectos sobre los que también hay que detenerse es en el cómo se va a establecer **la fecha y hora oficial**, que debe estar accesible en la sede electrónica, y que va a servir de referencia para, por ejemplo, el registro electrónico. En este caso va poder utilizarse **un servidor sincronizado con la ROA**, ya que con la acreditación del propio organismo titular de la sede electrónica es suficiente.

4.1.2 Actuación administrativa automatizada

Para determinar qué se entiende como actuación administrativa automatizada podemos remitirnos al Anexo de la LAECSP, dedicado a definiciones sobre conceptos reflejados en esta Ley. En él aparece definida como *"actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación."*

A modo de ejemplo, estos serían algunos casos que se amoldarían a esta definición:

- Expedición automática de recibos de presentación, por parte del registro electrónico de la Administración.
- Foliado automático de expedientes electrónicos.
- Emisión automática de copias auténticas de documentos electrónicos.
- Compulsas electrónicas.
- Digitalización de documentos en soporte papel.
- Migraciones y cambios de formato automáticos que podrían ser necesarios para cuestiones de archivo.
- Intercambio automático de datos entre Administraciones.

Según se indica en el art. 18 y art. 13.3.b) de la LAECSP, para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar según el caso el uso del **sello de órgano o el código seguro de verificación** como sistemas de firma electrónica. De ahí que en este apartado vamos a tratar estos dos sistemas de forma pormenorizada.

La LAECSP ha reservado el término **sello de órgano**, para aludir a los sistemas de autenticación de la actuación administrativa automatizada basados en certificados electrónicos, mientras que utiliza el término **código seguro de verificación**, para definir el medio alternativo de autenticación de la actuación automatizada, que resulta de traducir más fielmente al mundo electrónico el sello que se utiliza en la Administración en papel. La principal diferencia funcional estriba en que la verificación del sello electrónico se hace gracias al uso de las claves públicas incorporadas al certificado de sello electrónico, lo que requiere de la comprobación de la vigencia del certificado y admite la verificación electrónica automatizada, mientras que el código seguro de verificación precisa de la puesta a disposición del ciudadano de un sistema que permita su verificación, accesible a través de la sede electrónica de la Administración Pública autora.

SELLO DE ÓRGANO

El uso de certificados de sello de órgano va a facilitar la identificación electrónica de las Administraciones Públicas y va a permitir autenticar los documentos electrónicos que se deriven de la actividad administrativa automatizada, entendida como aparece definida en la LAECSP y como ya ha sido comentada.

De esta misma definición podemos sustraer que las Administraciones Públicas no pueden caer en el uso generalizado del sello de órgano en detrimento de, por ejemplo, la firma del funcionario competente, sino que es necesario que **cada Administración determine los supuestos y trámites en que el sello de órgano puede ser aplicado**, **para lo que deberá realizar una adecuada valoración**, de acuerdo con el principio de proporcionalidad, y sin que con ello se produzca una merma de garantías de los ciudadanos.

En este mismo sentido, resulta destacable que sólo se hace una referencia expresa del empleo del sello electrónico en la LAECSP, concretamente en el art. 30.3, referida a la posibilidad de automatizar el proceso de digitalización de documentos en soporte papel y obtención de las correspondientes copias electrónicas.

Al igual que ocurre con el certificado de sede electrónica, este tipo de certificados no puede ser implementado de cualquier manera, sino que van a tener que seguirse ciertas pautas en cuanto a los campos que lo forman. Ya en el art. 18.3 de la LAECSP se determina que este tipo de certificados tendrán que incluir el número de identificación fiscal y la denominación correspondiente de la Entidad en cuestión, pudiendo contener la identidad de la persona titular en el caso de sellos electrónicos de órganos administrativos. Además, y ya dentro de las especificaciones recogidas en el Esquema de identificación y firma electrónica, nos encontramos unas especificaciones más precisas del perfil de este tipo de certificados. Los campos que en él se determinan vienen clasificados, según su carácter, de la siguiente forma:

- Fijos:
  - Descripción del tipo de certificado, tomando en este caso el valor de "***sello electrónico***".
  - Nombre de la entidad suscriptora.
  - Número de identificación fiscal de entidad suscriptora.
- Opcionales:
  - Denominación de sistema o componente informático.
  - Dirección de correo electrónico.
  - Datos de identificación personal del titular del órgano administrativo:
    - Nombre de pila.

- Primer apellido.
- Segundo apellido.
- NIF o NIE.

Como ejemplo de implementación se adjunta un extracto del perfil del certificado de sello electrónico propuesto en el Esquema de identificación y firma.

2.3. Subject Alternate Names		**Si**	**Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa**
2.3.2.1. Tipo de certificado	Indica la naturaleza del certificado	F	Tipo= sello electrónico (String UTF8) Size = 31 2.16.724.1.3.5.2.1.*1*
2.3.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.2.1.*2*
2.3.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF suscriptora = NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.2.1.*3*
2.3.2.4. DNI/NIE del responsable	DNI o NIE del responsable del Sello	O	DNI/NIE responsable= ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.2.1.*4*
2.3.2.5. Denominación de sistema o componente	Breve descripción de la componente que posee el certificado de sello	O	Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no de lugar a ambigüedades. Denominación sistema = "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.2.1.*5*

Fig.16

Extracto del perfil de certificado de sello electrónico propuesto en el Esquema de identificación y firma

2.3.2.6. Nombre de pila	Nombre de pila del responsable del certificado	O	N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.2.1.6 Ej: "JUAN ANTONIO"
2.3.2.7. Primer apellido	Primer apellido del responsable del certificado	O	SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.2.1.7 ej: "DE LA CAMARA"
2.3.2.8. Segundo apellido	Segundo apellido del responsable del certificado	O	SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.2.1.8 ej: "ESPAÑOL"
2.3.2.9. Correo electrónico	Correo electrónico de la persona responsable del sello	O	Correo electrónico de la persona responsable del sello ej: juanantonio.delacamara.espanol@mpr .es (String) Size [RFC 5282] 128 OID: 2.16.724.1.3.5.2.1.9

A pesar de las singularidades que se han descrito a cerca de este tipo de certificados, este sistema de firma es, desde el punto de vista tecnológico, lo que hasta ahora se conocía como certificado de componente.

Además, y como complemento, se establece la obligación de que las Entidades Locales faciliten **un servicio de verificación de los sellos electrónicos** que sea público y accesible, tal como indica el art. 18.3 de la LAECSP. Sobre el funcionamiento de este tipo de servicios tratará el capítulo dedicado a **sistemas de verificación de firma**.

Como ya ocurría en el caso del certificado de sede electrónica, debido a que este tipo de certificados son de reciente creación, muchas Entidades han estado y están trabajando con otro tipo de certificados a la hora de ejercer su actuación por vía elec-

trónica, como por ejemplo, certificados de personas jurídicas, certificados de componentes informáticos, certificados de servidores seguros, etc. Sin embargo, éstos no son certificados tipificados y reconocidos como certificados de sello electrónico, por lo tanto no cumplen con los requerimientos que establece la legislación vigente, y tendrán que ser progresivamente sustituidos.

Hasta ahora hemos hecho una descripción genérica de las características de este tipo de certificados, pero hay ciertas peculiaridades que vendrán determinadas por el tipo de uso que la Entidad haga de ellos. A continuación exponemos los posibles escenarios y las peculiaridades asociadas a ellos.

ESCENARIO I: USO DE UN CERTIFICADO DE SELLO ELECTRÓNICO GENERAL PARA LA ENTIDAD LOCAL

Este caso de uso consiste en la emisión de un sello de aplicación general para todos los sistemas y servicios del Ayuntamiento o Diputación en cuestión. Este uso ha de acompañarse de procedimientos de seguridad complementarios que solventen la vulnerabilidad existente al replicar las claves e instalarlas en diferentes servidores de aplicaciones, asegurándonos de que ofrecemos las mayores garantías a los ciudadanos y administraciones receptores de las firmas electrónicas realizadas con dicho certificado.

En relación con esta situación, deben realizarse las siguientes recomendaciones:

- En general, debe realizarse un análisis de riesgos y de entorno, del que se derive la posibilidad de empleo de un sello para todos los usos, como ya se ha comentado anteriormente de forma general.

- Es necesario escoger un nombre adecuado al campo *"Denominación de sistema o componente informático"*, teniendo en cuenta que debería de ser generalista debido al uso global previsto por la entidad suscriptora, como por ejemplo *"Sello electrónico de la Diputación..."* o *"Sello electrónico del Ayuntamiento..."*.

De forma singular, es recomendable el empleo de un sello general para un organismo cuando nos encontramos en un contexto como es el intercambio de documentos electrónicos entre distintas administraciones, o a través de de entornos como la Red SARA.

ESCENARIO 2: USO DE UN CERTIFICADO DE SELLO ELECTRÓNICO POR CADA UNIDAD ORGÁNICA

Este caso se basa en la emisión de un sello electrónico asociado a la actividad administrativa de una unidad orgánica dentro de un Ayuntamiento o Diputación Provincial como puede ser un departamento o área específica (Ej.: Área de Hacienda, Área de Bienestar Social, Área de Cultura,...).

El certificado de sello identificaría y autenticaría a la unidad de forma unívoca, aunque el CIF correspondiente estaría asociado a la Entidad Local de la que dependiera.

A modo de ejemplo, el campo *"Denominación de sistema o componente informático"* podría tomar como valor: *"Sello electrónico del Área Tributaria"*, y como nombre de la entidad suscriptora: *"Ayuntamiento de..."*.

En relación con esta situación, no es conveniente llegar a un grado muy alto de disgregación de las unidades orgánicas, tanto por el coste que estos certificados suponen, como por el hecho de que hay Ayuntamientos que por su tamaño no necesitarían utilizar este tipo de certificados por áreas, y les bastaría con un certificado único para llevar a cabo su actividad administrativa.

ESCENARIO 3: USO DE CERTIFICADO DE SELLO ASOCIADO A UN SISTEMA DE INFORMACIÓN

Otra variante consiste en designar el certificado de sello electrónico a un sistema o plataforma en concreto. Un ejemplo claro para este tipo de uso sería un Registro Electrónico, de manera que por ejemplo el campo del certificado *"Denominación de*

sistema o componente informático" podría tomar el valor: *"Registro electrónico".*

ESCENARIO 4: DIPUTACIONES PROVINCIALES COMO PROVEEDORES DEL SERVICIO DE ADMINISTRACIÓN ELECTRÓNICA PARA AYUNTAMIENTOS

Las Diputaciones Provinciales van a tener que poner a disposición de los Ayuntamientos de su competencia las herramientas y sistemas necesarios para hacer realidad la Administración Electrónica. Evidentemente va a ser necesario que cuenten con un sello electrónico, pero aquí el dilema es si cada Ayuntamiento debe contar con un certificado de sello electrónico propio, o hacer uso del de la Diputación:

- Si van a contar con un **sello propio**, tendrán que valorar, en función de su tamaño, si disponer de un sello general o plantearse hacer uso de varios sellos en función de las áreas en las que estén distribuidos. Teniendo en cuenta el tipo de entidades que dependen de las Diputaciones Provinciales, para la mayoría, contar con un sello general sería suficiente. Además, a la hora de determinar el uso o no de múltiples sellos, hay que considerar el incremento de coste que esto implicaría. En este caso también nos encontraríamos con el problema asociado a la gestión de esos sellos, ya que la Diputación Provincial se tendría que responsabilizar de su custodia.

- En el caso de hacer **uso del certificado de sello electrónico propio de la Diputación Provincial**, la gestión y mantenimiento quedaría en manos de la propia Diputación a través de un convenio o fórmula semejante en el que la Entidad Local asumiera como propio este certificado. Esto supondría tener que ceder a la Diputación competencias propias de las Entidades Locales dependientes, con lo que ello supone (elaboración normativa, cesión económica para asumir esa competencia,...).

En ambos casos, se necesitará establecer un marco normativo, que determine las condiciones de uso y responsabilidades asociadas a estos certificados de sello electrónico. Estas consideraciones tendrán que estar incluidas dentro de un convenio más global que determinará las relaciones entre Diputación y Ente Local dependiente en materia de prestación de servicios de Administración Electrónica de forma delegada.

CÓDIGO SEGURO DE VERIFICACIÓN

En el art. 18.1 de la LAECSP se establece el código seguro de verificación (COVE) como posible sistema para utilizar como método de identificación y autenticación de las Instituciones Públicas en el ejercicio de sus competencias respecto a la actuación administrativa automatizada. Este sistema vincula a la Administración Pública o a la persona firmante con un documento, permitiendo en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente, lo que hace imprescindible implementar **un sistema telemático de consulta** mediante el cual se permita dicha comprobación. Este sistema está concebido como una herramienta vinculada a la comprobación de la autenticidad de las copias de los documentos administrativos generados electrónicamente.

Si nos remitimos al art. 20 del R.D. 1671/2009, estos códigos deberán garantizar, además de todos los requerimientos puramente burocráticos:

"a) El carácter único del código generado para cada documento.

b) Su vinculación con el documento generado y con el firmante.

c) Asimismo, se debe garantizar la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento."

No tenemos que olvidar que esta normativa es de carácter estatal, pero nos puede ayudar a conocer la tendencia que se seguirá a nivel local.

A priori este sistema puede parecer, frente al certificado de sello electrónico, un método rudimentario e incluso innecesario existiendo el ya nombrado, pero entenderemos mejor su necesidad exponiendo un caso práctico, como el hecho de imprimir documentos originales electrónicos. En este caso, para comprobar la autenticidad del documento va a ser necesaria alguna *marca* o distintivo que lo haga posible, ya que al imprimir perdemos la firma electrónica que lo acompaña. De hecho, así lo prevé la LEACSP, en su art. 30.5: *"Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente* ***tendrán la consideración de copias auténticas siempre que incluyan la impresión de***

un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad *mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora*", lo que ha supuesto el espaldarazo definitivo al código seguro de verificación.

En el caso del Boletín Oficial de Castilla y León (BOCYL), el COVE aparece incluido en cada una de las páginas de cada documento, como aparece destacado en la siguiente imagen.

BOCYL Boletín Oficial de CASTILLA Y LEÓN

Núm. 211 Lunes, 11 de octubre de 2010 Pág. 121.412

I. COMUNIDAD DE CASTILLA Y LEÓN

C. OTRAS DISPOSICIONES

CONSEJO DE CUENTAS DE CASTILLA Y LEÓN

RESOLUCIÓN de 28 de octubre de 2009, del Presidente del Consejo de Cuentas de Castilla y León, por la que se publica Acuerdo por el que se nombra la Comisión de Valoración que ha de resolver la convocatoria del concurso ordinario efectuada por Acuerdo del Pleno 44/2009, de 11 de junio.

El Pleno del Consejo de Cuentas de Castilla y León, en su sesión de 19 de octubre de 2009, adoptó el Acuerdo 98/2009, cuyo texto es el siguiente:

"De conformidad con la base séptima de la convocatoria aprobada en virtud del Acuerdo 44/2009, de 11 de junio (B.O.C. y L." 26 de junio de 2009), del Pleno del Consejo de Cuentas de Castilla y León, y una vez realizadas las oportunas designaciones, el Pleno nombra la Comisión de Valoración, que estará formada por:

COMISIÓN TITULAR:
Presidenta: Virtudes de la Prieta Miralles.
Vocales: Manuel Pérez Carbajosa.
Yolanda Martínez González.
Juan Carlos de la Rosa Muñoz.
Fortunato Rodicio Martín.
Secretario: Juan José Castrillo Serrano.

COMISIÓN SUPLENTE:
Presidente: Javier Domínguez Domínguez.
Vocales: Raimundo Fombellida Aragón.
Luis Mariano Tapias Esteban.
Esteban Riera González.
Milagros Ruiz Mosiares.
Secretario: Manuel M.ª Marcos Álvarez.

Publíquese el presente Acuerdo en el "Boletín Oficial de Castilla y León".

Palencia, 28 de octubre de 2009.

El Presidente,
Fdo.: PEDRO MARTÍN FERNÁNDEZ

http://bocyl.jcyl.es D.L.: M-1/1977 – ISSN: 0212-033X

CV: BOCYL-D-11102010-2 → Código de verificación del documento

Fig.17

COVE en un documento electrónico publicado en el BOCYL

Además, en el portal web del BOCYL, también se ha habilitado un sistema con el que poder cotejar los documentos emitidos a través del COVE, como se muestra a continuación.

Fig.18

Página habilitada por la Junta de Castilla y León para el cotejo de documentos electrónicos pertenecientes al BOCYL

De forma complementaria, junto con el código seguro de verificación, los documentos suelen ir acompañados de un **código PDF** (Portable Document Format), que consiste en una serie de puntos que se incluyen en el documento impreso, de manera análoga a los códigos de barras, y que contienen la misma información que la contenida en el COVE, con el valor añadido de ser susceptible a ser capturada con un lector laser. La lectura de los códigos mediante pistola láser evita la labor de grabación manual de los datos y permite automatizar el proceso de cotejado de estos documentos.

Es aconsejable incluir en los documentos ambos códigos ya que:

- Los usuarios, generalmente, no van a estar en disposición de un lector láser para proceder al cotejo, de ahí que en su mayoría utilicen el COVE.

- Las Entidades Locales, necesitarán tramitar un gran volumen de cotejos, con lo que se hace aconsejable el que adquieran este tipo de lectores, y por tanto que incluyan estos códigos PDF en los documentos.

Tradicionalmente los códigos de barras almacenan información en su dimensión horizontal, utilizando la vertical para proveer de redundancia para:

- Resolución de errores por códigos parcialmente dañados.

- Flexibilidad a la hora de leer los códigos, respecto a la orientación y los límites.

Actualmente, se ha evolucionado hacia códigos que aprovechan las dos dimensiones para almacenar la información, haciendo uso de nuevas simbologías basadas en la definición de una matriz de renglones y columnas de datos codificados, entre las cuales podemos encontrar la especificación PDF 417, que está siendo utilizada, entre otras Administraciones, por la Agencia Tributaria.

Este tipo de código de barras puede almacenar como máximo 1800 caracteres alfanuméricos ASCII o 1100 códigos binarios por cada símbolo (cada rectángulo en forma de *nube de puntos*).

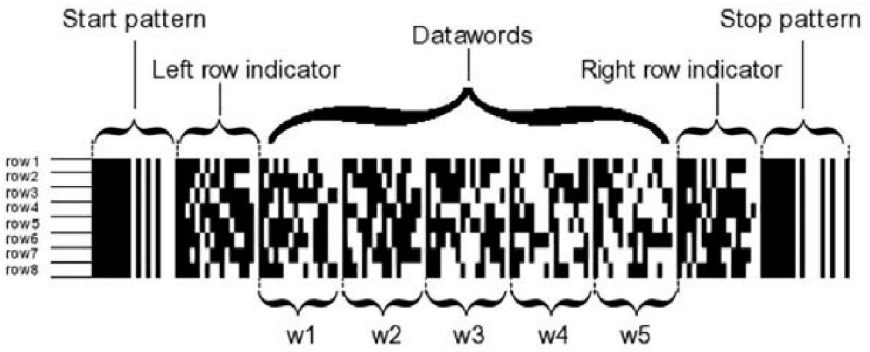


Fig.19

Estructura utilizada en la especificación PDF 417

Otro ejemplo de código bidimensional es el QR-CODE (Quick Response Barcode), que al igual que el anterior permite almacenar información en la matriz de puntos, pero cuenta con una mayor capacidad (un máximo 4296 caracteres alfanuméricos ASCII). Esta matriz se caracteriza por los tres cuadrados que se encuentran en sus esquinas, y que permiten que el lector detecte la posición del código. La Junta de Castilla y León está utilizando este tipo de códigos, y en ellos se almacena la información administrativa permitente.

Fig.20

Ejemplo de uso del código QR-CODE en la Junta de Castilla y León

4.1.3 Personal al servicio de las Administraciones Públicas

Otra figura que es necesaria trasladar al marco electrónico que pretendemos conformar, es la identidad del empleado al servicio de la Administración Pública. Esta nueva figura viene referenciada en la LAECSP a través de:

- art. 13.3.c), en el que la firma electrónica del personal al servicio de las Administraciones Públicas aparece entre los sistemas de identificación y autenticación electrónica de los documentos que estas Entidades produzcan.

- art. 19, dedicado en su totalidad a la firma electrónica del personal al servicio de las Administraciones Públicas.

En ellos se establece como forma de identificación de esta figura **el certificado de empleado público**, pudiendo hacerse uso para tal efecto los sistemas de firma electrónica incluidos en el DNIe personal del empleado.

Actualmente, los empleados públicos vienen utilizando, para la autenticación e identificación electrónica en su ámbito laboral, certificados reconocidos de persona física, entre los que se encuentra el DNIe y sistemas basados en la utilización de claves concertadas (Ej.: usuario y password), cuyo uso se determina en función del caso y siempre siguiendo el criterio de proporcionalidad. Sin embargo, el uso de estos certificados de persona física, además de establecerse como un mecanismo voluntario por parte del empleado, no determinan la vinculación directa entre dicho empleado y el puesto que ocupa en la organización a la que esté adscrito, y por tanto tampoco aparecerá esta vinculación en las firmas electrónicas a partir de los cuales se generen.

Como en casos anteriores, y conforme a lo previsto en el art. 19 de la LAECSP, se plantea la necesidad de disponer de perfiles de certificados específicos para el personal al servicio de las Administraciones Públicas, que vinculen al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

Pero este tipo de certificados no van a poder ser definidos de cualquier manera, sino que lo más adecuado es regirse por las directrices que a este respecto también se han definido en el Esquema de identificación y firma electrónica, a efectos de garan-

tizar la interoperabilidad entre las distintas Administraciones Públicas. Para ello, se utiliza un certificado tecnológicamente igual que el de las personas físicas pero con ciertos atributos específicos, como ocurre en los casos anteriormente comentados. En este caso se definen una serie de campos que se dividen, según su carácter, de la siguiente forma:

- Fijos:
  - Descripción del tipo de certificado, tomando en este caso el valor de "***certificado de empleado publico***".
  - Datos de identificación personal de titular del certificado:
    - Nombre de pila.
    - Primer apellido.
    - Segundo apellido.
    - DNI o NIE.
  - Nombre de la entidad en la que está suscrito el empleado.
  - Número de identificación fiscal de entidad.
- Opcionales:
  - Unidad a la que está adscrito el cargo o puesto que desempeña el empleado público.
  - Cargo o puesto de trabajo.
  - Número de identificación de personal (NIP, NRP,...).
  - Dirección de correo electrónico.

Como ejemplo de implementación, se adjunta un extracto del perfil del certificado de empleado público propuesto por el Esquema de identificación y firma.

2.4. Subject Alternate Names		**SI**	**Lugar donde se contemplarán los valores establecidos para la Identidad Administrativa**
2.4.2.1. Tipo de certificado	Indica la naturaleza del certificado	F	Tipo= certificado electrónico de empleado público (String UTF8) Size = 31 OID: 2.16.724.1.3.5.3.1.1
2.4.2.2. Nombre de la entidad suscriptora	La entidad propietaria de dicho certificado	F	Entidad Suscriptora = ej: MINISTERIO DE LA PRESIDENCIA (String UTF8) Size = 80 OID: 2.16.724.1.3.5.3.1.2
2.4.2.3. NIF entidad suscriptora	Número único de identificación de la entidad	F	NIF suscriptora = NIF entidad suscriptora ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.3.1.3
2.4.2.4. DNI/NIE del responsable	DNI o NIE del responsable	F	DNI/NIE responsable= ej: 00000000G (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.1.4
2.4.2.5. Número de identificación de personal	Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP	O	Número identificativo = ej: A02APE1056 (String UTF8) Size = 10 OID: 2.16.724.1.3.5.3.1.5
2.4.2.6. Nombre de pila	Nombre de pila del responsable del certificado	F	N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.3.1.6 Ej: "JUAN ANTONIO"

Fig.21

Extracto del perfil de certificado de empleado público propuesto por el Esquema de identificación y firma

2.4.2.7. Primer apellido	Primer apellido del responsable del certificado	F	SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.3.1.7 Ej: "DE LA CAMARA"
2.4.2.8. Segundo apellido	Segundo apellido del responsable del certificado	F	SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.3.1.8 Ej: "ESPAÑOL"
2.4.2.9. Correo electrónico	Correo electrónico de la persona responsable del certificado	O	Correo electrónico de la persona responsable del certificado ie: juanantonio.delacamara.espanol@mpr .es (String) Size [RFC 5282] 128 OID: 2.16.724.1.3.5.3.1.9
2.4.2.10. Unidad organizativa	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado	O	Unidad = ej: SUBDIRECCION GENERAL DE PROCESO DE DATOS (String) Size [RFC 5282] 128 OID: 2.16.724.1.3.5.3.1.10
2.4.2.11. Puesto o cargo	Puesto desempeñado por el suscriptor del certificado dentro de la administración.	O	Puesto = ej: ANALISTA PROGRAMADOR (String) Size [RFC 5282] 128 OID: 2.16.724.1.3.5.3.1.11

El certificado de empleado público tiene una importante problemática asociada. Hay que tener en cuenta, que un certificado de este tipo contiene, como ya hemos visto, ciertos campos asociados al cargo que el poseedor del certificado ocupa en la Administración Pública, pero este cargo no tiene porque ser ejercido por tiempo indefinido, ya que el empleado puede promocionar, darse de baja, ostentar un interinidad o un contrato de tiempo definido,...De hecho, estas modificaciones asociadas al cargo del empleado no son ni mucho menos puntuales, de manera que con relativa frecuencia, en el caso de optar por **incluir los datos relativos al puesto que ocupa en**

el propio certificado, será necesario llevar a cabo las revocaciones pertinentes. Esto conlleva un aumento del número de operaciones asociadas a la gestión de estos certificados, lo que dificulta las tareas de gestión, y un aumento del tamaño de las CRLs. Esta realidad ha hecho que aparezcan una serie de campos opcionales asociados a esta caracterización del puesto del empleado, para así dotar a cada Entidad Local de cierta autonomía a la hora de determinar los atributos asociados a este tipo de certificados. Es decir, que se ha dejado en manos de la Entidad la elección del grado de precisión con el que se va a describir al poseedor de este tipo de certificados respecto a su relación laboral con la Administración Pública.

A modo de ejemplo, en el ámbito de la AGE, a través del R.D. 1671/2009, sólo se definen los campos obligatorios que deben aparecer en este tipo de certificados electrónicos, de acuerdo con el Esquema de identificación y firma electrónica, dejando abierto a cada Entidad el uso del resto de campos.

Una manera de resolver el problema asociado a la inclusión de todos los datos en el propio certificado, es incluir sólo parte de ellos en el propio certificado, como podrían ser los campos mínimos antes señalados, dejando a disposición de las aplicaciones que lo necesiten los datos concretos del puesto o cargo en **un directorio**. Esta solución evita la problemática de revocaciones y nuevas emisiones de certificados, pero requiere un mantenimiento ágil del directorio.

Cualquiera de las dos soluciones planteadas es factible tanto legal como técnicamente, y ambas podemos encontrarlas implementadas en Administraciones Públicas españolas, la diferencia primordial radica en los mecanismos de gestión a utilizar durante el ciclo de vida de los certificados. La opción que se adopte es necesario que venga acompañada de un razonamiento previo acerca de la problemática de cada Entidad, de manera que si se opta por la primera opción, hay que tener en cuenta que se dispondrá de toda la información en el certificado, lo que requerirá de la intervención, y por tanto de la dependencia, de la autoridad de certificación para gestionar las revocaciones y nuevas emisiones de certificados que van a ser necesarias. En el caso de decantarse por la segunda opción, los datos residirán en un directorio, evitando así la intervención de la autoridad de certificación emisora, esto requerirá por otro lado que sea necesario que este directorio se mantenga actualizado y disponible en todo momento para las aplicaciones que lo utilicen.

A continuación se exponen tres posibles situaciones en las que pueden estar los empleados públicos y que se salen del caso general correspondiente a un empleado público que pertenece a un único organismo y que únicamente ostenta un cargo:

CASO I: EMPLEADOS PÚBLICOS VINCULADOS A VARIOS ÓRGANOS DEPENDIENTES DE UNA MISMA ENTIDAD

Existen empleados públicos, que debido a su cargo o puesto de trabajo, ostentan otros cargos en otros organismos dependientes o vinculados al organismo principal. En relación con esta situación, se deberían diseñar las aplicaciones de forma que estas personas no tengan que disponer de un certificado para cada organismo, sino que puedan emplear un único certificado para sus actuaciones como firmantes en todos ellos. Para ello, se puede hacer uso de un certificado que recoja los campos mínimos, apoyado por la posibilidad de acceder a un directorio con el resto de la información relativa al cargo, en función de las actuaciones que en cada momento realice.

CASO II: EMPLEADOS PÚBLICOS DE MÚLTIPLES ORGANISMOS INDEPENDIENTES

En este caso se encontrarían las personas que, por razón de su rol o función, se encuentran habilitados para actuar en diferentes órganos, como sucede por ejemplo con los secretarios, interventores y tesoreros, que pueden actuar en diversos organismos, en función de las necesidades.

Esta singularidad es similar a la anteriormente presentada, con la diferencia de que, en este caso, por tratarse de funciones transversales a diversos departamentos y, en algún caso, a diversas administraciones, resulta recomendable centralizar la emisión y gestión de los certificados en algún organismo externo (Ej.: el colegio correspondiente o la unidad administrativa oportuna). De esta manera no es necesario posteriormente emitir certificados para estos roles, en cada uno de los órganos u organismos en que estén temporalmente adscritos.

4.2 IDENTIFICACIÓN DE LOS CIUDADANOS

Hasta ahora hemos ido desgranando las necesidades identificativas que, como Ayuntamiento o Diputación, tenemos que poner en marcha tanto de cara al exterior como al interior. Del mismo modo, los agentes que interactúan con nosotros (ciudadanos y empresas) tienen que disponer y poder utilizar una serie de recursos que les permita identificarse a la hora de utilizar los servicios que se pongan en marcha, bajo el principio de proporcionalidad.

Según el art. 13 de la LAECSP, las Administraciones Públicas admitirán sistemas de firma electrónica conforme a lo dispuesto por la LFE, permitiendo a los ciudadanos utilizar:

a) **En todo caso**, **el DNIe para personas físicas**.

b) **Sistemas de firma electrónica avanzada**, incluyendo los basados **en certificados reconocidos**, admitidos por las Administraciones Públicas **para personas físicas**, **personas jurídicas y entes sin personalidad jurídica**. Tratándose de firma electrónica reconocida, las Administraciones están también obligadas a aceptarla, siempre y cuando la autoridad de certificación dé acceso **gratuito** a su lista de certificados revocados (CRL).

   La Ley faculta a las Administraciones Públicas a decidir qué otros sistemas de firma electrónica avanzada aceptan, de ahí que en el art. 15 de la LAECSP se indique que éstas deberán publicar y tener accesible la relación de sistemas que admiten.

   También se recoge la posibilidad de que **los entes sin personalidad jurídica** puedan ser titulares de certificados electrónicos para poder relacionarse con la Administración. Tanto en este caso, como en el de las personas jurídicas, y de acuerdo con la LFE, sus certificados deberán incorporar la identidad de la persona que solicita y se responsabiliza de custodiar el certificado.

   En todo caso los certificados deben de tener incorporado el NIF de su titular, ya sea persona física, jurídica o ente sin personalidad jurídica.

c) Se posibilita la admisión de **otros sistemas de firma electrónica**, incluso la de aquellos que no se basen en sistemas de criptografía asimétrica y por tanto no impliquen la existencia de certificados electrónicos. Por tanto, se podrán utilizar por ejemplo, claves concertadas entre las partes, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que se determinen en cada caso. En este caso, y según el art. 16 de la LAECSP, las Administraciones Públicas podrán determinar, teniendo en cuenta los datos e intereses de los afectados, y siempre de forma justificada, los supuestos y condiciones de utilización de estos sistemas, mientras se garantice la integridad y el no repudio por ambas partes.

Cuando una Administración Pública ponga a disposición de los ciudadanos un servicio tendrá que determinar, según la naturaleza del mismo y bajo criterios de proporcionalidad, el tipo de identificación que es exigible, de ahí la importancia de realizar el análisis de riesgos que ya ha sido comentado en varios puntos de este documento. Tenemos que evitar tender a un criterio de máximos, es decir a no exigir a los ciudadanos un certificado reconocido si no es necesario.

4.2.1 Identificación de la persona física

Como podemos inferir de lo anterior, las Entidades Locales, a la hora de poner en marcha un servicio en el que se tenga que interoperar con personas físicas, tienen que determinar los requerimientos necesarios para garantizar la integridad y no repudio por ambas partes de los procedimientos o trámites que se realicen. En base al estudio previo que se realice del servicio, se podrá indicar como medio de identificación y autenticación algunos de los siguientes:

- DNI electrónico, en todo caso. La LFE, en su art. 15, establece la obligación a todas las personas físicas o jurídicas, públicas o privadas a reconocer la eficacia del DNIe para acreditar la identidad y los demás datos personales del titular que conste en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos. La LAECSP se limita a recordar esta obligación para las Administraciones Públicas.

- Firma electrónica reconocida.
- Firma electrónica avanzada.
- Otros sistemas de firma, que no necesariamente tienen que ser de carácter criptográfico (Ej.: claves concertadas).

En la siguiente figura aparece una imagen con la composición de las pantallas que recogen la información general y parte de la detallada de un certificado de persona física.

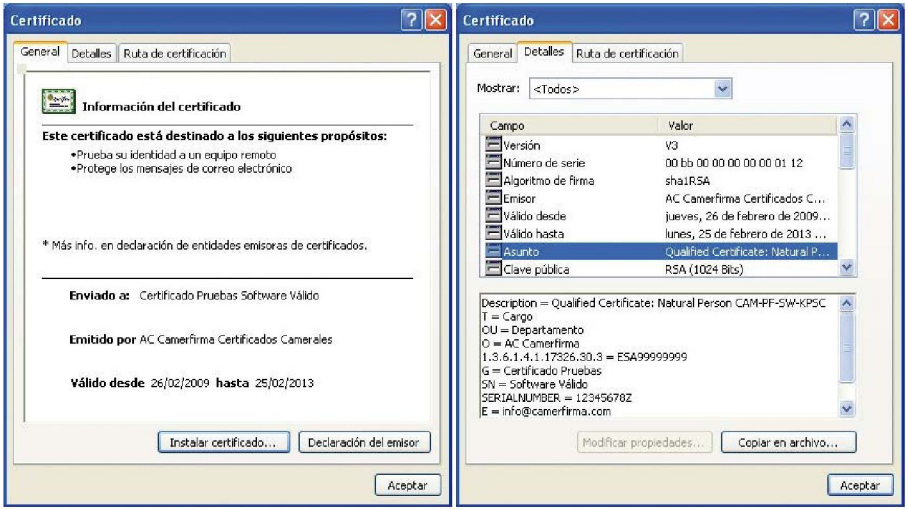


Fig.22

Ejemplo de certificado de persona física emitido por Camerfirma

4.2.2 Identificación de la persona jurídica

Cuando una persona jurídica pretenda hacer uso de un servicio puesto en marcha por una Administración Púbica, ésta podrá utilizar, según el tipo de servicios:

- Firma electrónica reconocida.
- Firma electrónica avanzada.
- Otros sistemas de firma, que no necesariamente tienen que ser de carácter criptográfico (Ej.: claves concertadas).

Pero en este caso en concreto, la expedición del certificado va a requerir satisfacer una serie de requisitos adicionales respecto a la expedición en el caso de personas físicas.

Según el art. 7 de LFE, *"podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos"*. De manera que queda en manos de la persona física solicitante tanto la custodia de datos de creación de firma asociada a cada certificado como la responsabilidad que implica, de ahí que en el certificado se incluya su identificación.

Además la persona jurídica podrá incluir limitaciones en el uso del certificado, de manera que sólo sea utilizado para los fines con los que se pretendía usar, de forma que si se transgredieran esos límites, las consecuencias recaerían sobre la persona física solicitante, a no ser que fuese asumido por la persona jurídica como propio.

En el caso de firma electrónica reconocida, se hace necesario que los prestadores de servicios de certificación, además de comprobar la identidad y circunstancias del firmante y verificar la información contenida en el certificado, deberán comprobar los datos relativos a la constitución y personalidad jurídica, y a la extensión y vigencia de las facultades de representación del solicitante. Estas consideraciones son definidas en el art. 13 de la LFE, al que se le ha dado una nueva redacción en el art 5 de la LMISI, con el objetivo de flexibilizar las obligaciones de los prestadores de servicios de certificación y eliminar cargas excesivas.

A continuación se muestra una imagen compuesta por las capturas de pantalla correspondientes a la ventana que recoge la información general y la correspondiente a la información más detallada de un certificado de persona jurídica.

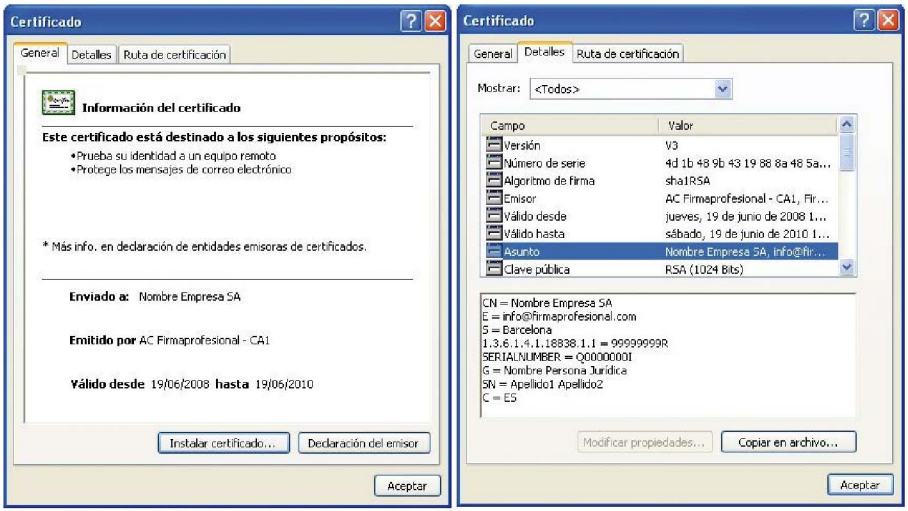


Fig.23

Ejemplo de certificado de persona jurídica emitido por Firma Profesional

4.2.3 Identificación de una entidad sin personalidad jurídica

La expedición de este tipo de certificados viene definida en la disposición adicional tercera de la LFE. En ella se limita su expedición a las entidades referidas por el art. 33 de la Ley General Tributaria para su utilización en el ámbito tributario, en los términos que establezca el Ministerio de Hacienda.

En esta categoría de entidades se engloba a las herencias yacentes, comunidades de bienes y demás entidades que, carentes de personalidad jurídica, constituyen una unidad económica o un patrimonio separado, susceptibles de imposición.

4.2.4 Representación mediante funcionario público

Hay que tener en cuenta que muchos ciudadanos no disponen actualmente de un sistema de firma electrónica para poder llevar a cabo un trámite telemático con su

Ayuntamiento o Diputación, pero tan habitual como esto, va a ser el caso de personas que no disponen de los conocimientos o habilidades necesarias para poder utilizar estas nuevas herramientas a las que van a tener acceso, como queda reflejado en el art. 4.b) sobre el principio de proporcionalidad. Por ello, en el art. 22 de la LAECSP aparece determinada una nueva forma de representación de estos ciudadanos mediante un funcionario público. Para llevar a cabo este tipo de representación, la Entidad Local debe poner a disposición del ciudadano los medios técnicos y humanos que este sistema de representación requiere, y que se concretan en:

- Una localización física a la que los ciudadanos puedan dirigirse para acceder a esos servicios telemáticos (Ej.: oficina de atención presencial).

- Un equipo informático con el hardware (Ej.: lector de tarjetas) y software necesario.

- Un funcionario público dotado de los sistemas de firma electrónica necesarios para su identificación.

Además, la Administración necesita **habilitar al conjunto de empleados públicos** que van llevar a cabo esa tarea de representación, incorporándolos a un **registro de funcionarios habilitados** que mantendrá actualizado.

Los ciudadanos por su parte, tendrán que dirigirse a esa **oficina de atención presencial** con la documentación que le permita identificarse, es decir con su DNI, y dar su consentimiento expreso, debiendo quedar constancia de ello para los casos en los que se produzca alguna discrepancia o litigio, de manera que deberán firmar un documento que permita acreditar este consentimiento.

4.2.5 Representación mediante un tercero

La LAECSP también contempla, en su art. 23, la posibilidad de que un ciudadano realice determinadas transacciones a través de un tercero (persona física o jurídica) que lo represente. Para ello ese tercero debe contar con **una habilitación** en la que deberán

aparecer especificadas **las condiciones y obligaciones a las que se comprometen** los que así adquieren la condición de representantes. Por su parte, las Administraciones Públicas podrán requerir en cualquier momento estas acreditaciones.

En el caso de certificados reconocidos que reflejen estas relaciones de representación, el prestador de servicios, según el art. 13 de la LFE (al que se le ha dado una nueva redacción en el art. 5 de la LMISI), deberá exigir la acreditación que fundamente estas circunstancias.

Además, y como complemento, en el R.D. 1671/2009, en el que se prevé un régimen especifico que facilita la actuación en nombre de terceros, se establece la creación de un **registro electrónico de apoderamientos**, como nuevo mecanismo de acreditación, en el que se podrán hacer constar las representaciones que se otorguen a terceros, y que permitirá comprobar la representación que ostentan quienes actúen electrónicamente en nombre de terceros. Debido al ámbito de aplicación de este R.D., la creación de este registro va a permitir centralizar las comprobaciones que en este sentido requieran todas las entidades englobadas en la AGE. En el ámbito local, debemos tener en consideración estas medidas para su posible aplicación, sobre todo en aquellas entidades que por su dispersión u organización les pueda ser útil su implementación.

5

5 IDENTIFICACIÓN EN OTROS ELEMENTOS DE LA ADMINISTRACIÓN ELECTRÓNICA

La constitución de la **sede electrónica** de una Entidad Local, permite que ésta ponga a disposición de los ciudadanos un punto de acceso electrónico a los servicios del Ayuntamiento. Es por tanto **un elemento esencial**, debido a que es la puerta de entrada a nuestros Ayuntamientos y Diputaciones desde cualquier punto con conexión a Internet y en cualquier momento del día.

Pero para que podamos incorporarnos plenamente a la Administración Electrónica, tenemos que dotar a nuestras Administraciones Públicas tanto de estas sedes electrónicas, como de una serie de servicios y herramientas que las complementen. A su vez, estas aplicaciones y servicios van a necesitar estar dotados de los sistemas de identificación y firma electrónica que se han ido comentado durante este documento, por lo tanto, en este apartado se va a ir determinando los elementos y servicios que tenemos o podemos poner en marcha y los requerimientos, que respecto a identificación y autenticación, debemos de satisfacer.

5.1 SISTEMAS DE VERIFICACIÓN DE FIRMA ELECTRÓNICA

Para encontrar una definición de este tipo de sistemas tenemos que dirigirnos al art. 25.2 de la LFE, donde se refiere a ellos como "un programa o sistema informático que sirve para aplicar los datos de verificación de firma", entendidos estos como códigos o claves criptográficas públicas.

La implementación de estos dispositivos requiere que, según el art. 25.3 de la LFE, el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

"a) *Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.*

b) *Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.*

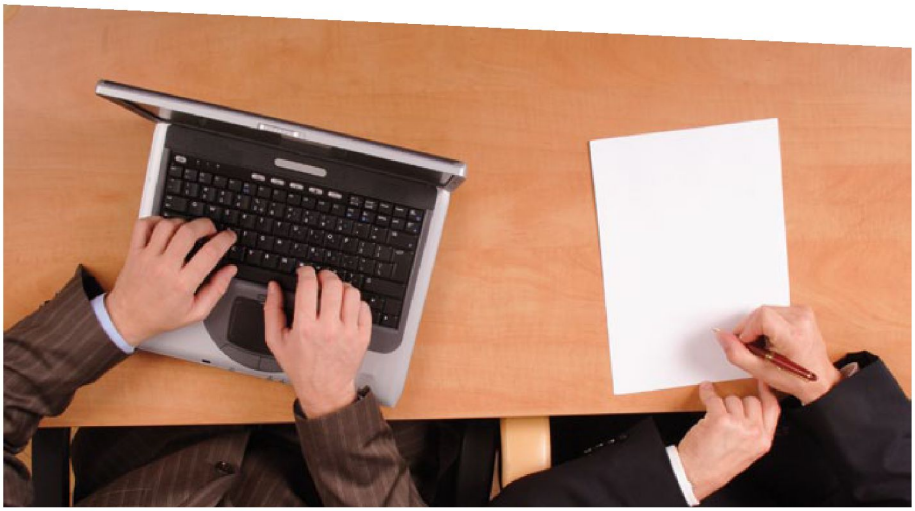
c) *Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.*

d) *Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.*

e) *Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.*

f) *Que pueda detectarse cualquier cambio relativo a su seguridad."*

Estar en disposición de este tipo de servicios, permite que los ciudadanos puedan comprobar de forma inmediata, la validez de las firmas y certificados electrónicos



que acompañan a los documentos electrónicos, lo que directamente va a afianzar la confianza de estos ciudadanos en el uso del medio electrónico como canal para relacionarse con las Administraciones Públicas.

De hecho, la importancia de incorporar este tipo de servicios aparece recogida en el art. 6 del R.D. 1671/2009, en el que se establece que entre los servicios accesibles desde la sede electrónica de cada Entidad se encuentren:

- *art. 6.1.d) "**Sistema de verificación de los certificados de la sede**, que estará accesible de forma directa y gratuita."*

- *art. 6.2.h) "**Verificación de los sellos electrónicos** de los órganos u organismos públicos que abarque la sede."*

Esto requiere que los prestadores de servicios de certificación, como queda reflejado en el art. 18 de LFE, deban garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados. Este aspecto también queda reflejado en el art. 23 R.D. 1671/2009, donde se indica que *"los prestadores de servicios de certificación deben facilitar a las plataformas públicas de validación que se establezcan, acceso electrónico y gratuito para la verificación de la vigencia de los certificados asociados a sistemas utilizados por los ciudadanos, la Administración General del Estado y sus organismos públicos"*.

Básicamente, este tipo de servicios funcionan de la siguiente manera:

- El ciudadano, a través del servicio puesto en marcha desde la sede electrónica de la Entidad Local, envía una petición de validación del certificado o de la firma al servidor que para este fin tiene habilitado un determinado proveedor de servicios de certificación.

- Una vez recibida esta petición, el proveedor consulta sus fuentes, conocidas como CRLs.

- Tras la consulta, el proveedor envía al ciudadano la información relativa al estado actual del certificado.

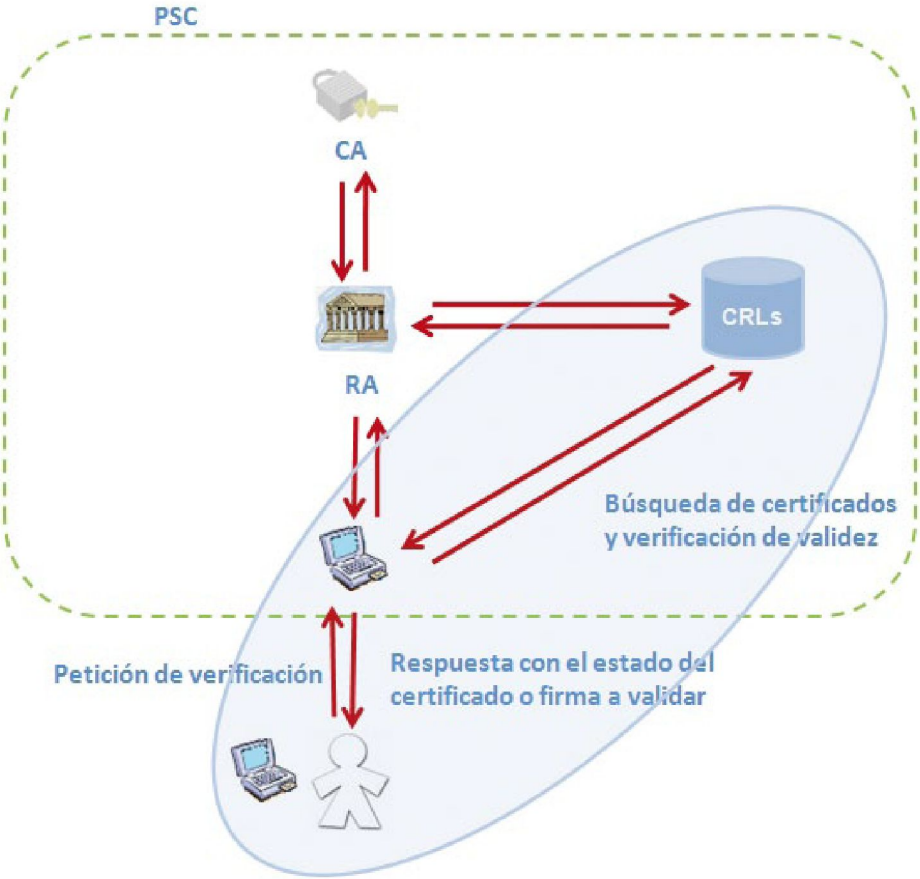


Fig.24

Funcionamiento de un dispositivo de verificación de firma

En este mismo contexto hay que introducir un nuevo concepto, **las plataformas de validación de certificados electrónicos y de firma electrónica**, que aparece definido en el art. 20 del ENI, como *"servicios de confianza de las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, que proporcionan servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las Administraciones públicas"*.

La AGE, como respuesta a la imposición que la LAECSP hace en su art. 21 de poner

en marcha una **plataforma de verificación** del estado de revocación a todos los certificados admitidos en el ámbito de las Administraciones Públicas, ha implementado la plataforma **@Firma**[8], que supone un impulso a la implantación de la firma electrónica y el DNIe. Con ello se ha establecido un servicio centralizado y gratuito que permite a las aplicaciones de Administración Electrónica acceder a servicios de validación de todos los certificados reconocidos y a los de verificación de firmas electrónicas. Ésta plataforma lleva siendo usada por la Junta de Castilla y León desde 2005.

Con el uso de esta plataforma, o de plataformas de este mismo tipo, se unifica el sistema de peticiones antes comentado, ya que es como si se añadiera una capa sobre los proveedores de servicios de certificación que nos permite trabajar con ellos de forma transparente.

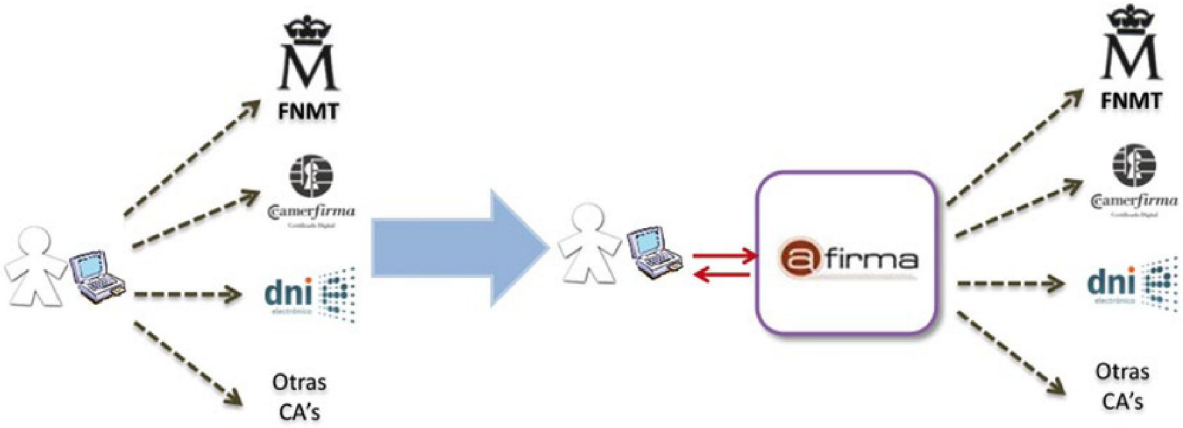


Fig.25

Esquema del proceso de verificación sin y con una plataforma de verificación

5.2 REGISTRO ELECTRÓNICO

El registro electrónico es uno de los elementos de la Administración Electrónica más implantados en la actualidad, que encontraremos alojado en las sedes electrónicas de las Administraciones Públicas. Este hecho es consecuencia del apoyo normativo que ha recibido, y que se remonta a la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante Ley 30/1992), donde en su art. 38 ya se recoge que los registros genera-

8. Para más información sobre @firma, se puede acceder al portal del Consejo Superior de Administración Electrónica (www.csae.map.es).

les, así como todos los registros que las Administraciones Públicas establezcan para la recepción de escritos y comunicaciones de los particulares o de órganos administrativos, deberán instalarse en soporte informático.

Su espaldarazo definitivo ha venido de la mano de la LAECSP, por la que, según el art. 24, las Administraciones Públicas **tienen la obligación de crear registros electrónicos** para la recepción y remisión de solicitudes, escritos y comunicaciones. Además, no hay que olvidar que el registro electrónico forma parte del grupo de elementos imprescindibles para alcanzar el tercer nivel de los cinco definidos en el **modelo de sofisticación**, que se utiliza en el ámbito europeo para medir la **disponibilidad online de servicios**. En él se contempla la posibilidad del envío a la Administración de los formularios por vía electrónica o la respuesta personalizada por parte de la Administración a consultas de los ciudadanos.

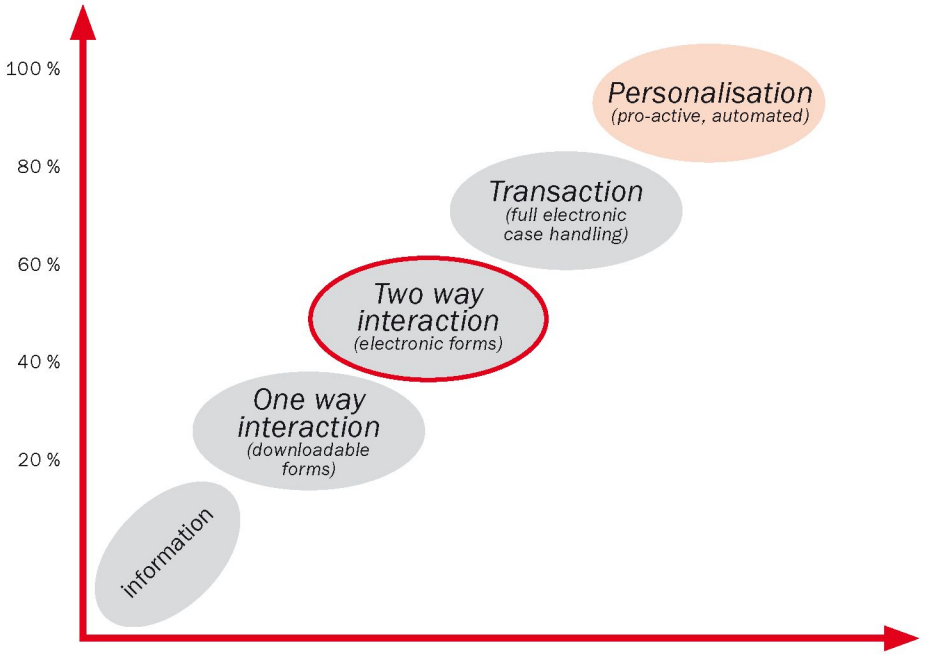


Fig.26

Etapas del modelo de sofisticación[9]

9. Fuente: *"The User Challenge Benchmarking The Supply Of Online Public Services"* publicado en septiembre de 2007 por Capgemini para la Comisión Europea (Directorate General for Information Society and Media).

Como servicio, el registro electrónico va a permitir flexibilizar ostensiblemente las relaciones entre ciudadano y Administración, ya que es el punto de intercambio de información más importante entre ellos. En la siguiente figura se muestra el diagrama funcional del registro electrónico que facilita el Centro Nacional de Referencia de Aplicación de las TIC basadas en fuentes abiertas (CENATIC), y que puede servir para comprender mejor el funcionamiento de este tipo de aplicaciones.

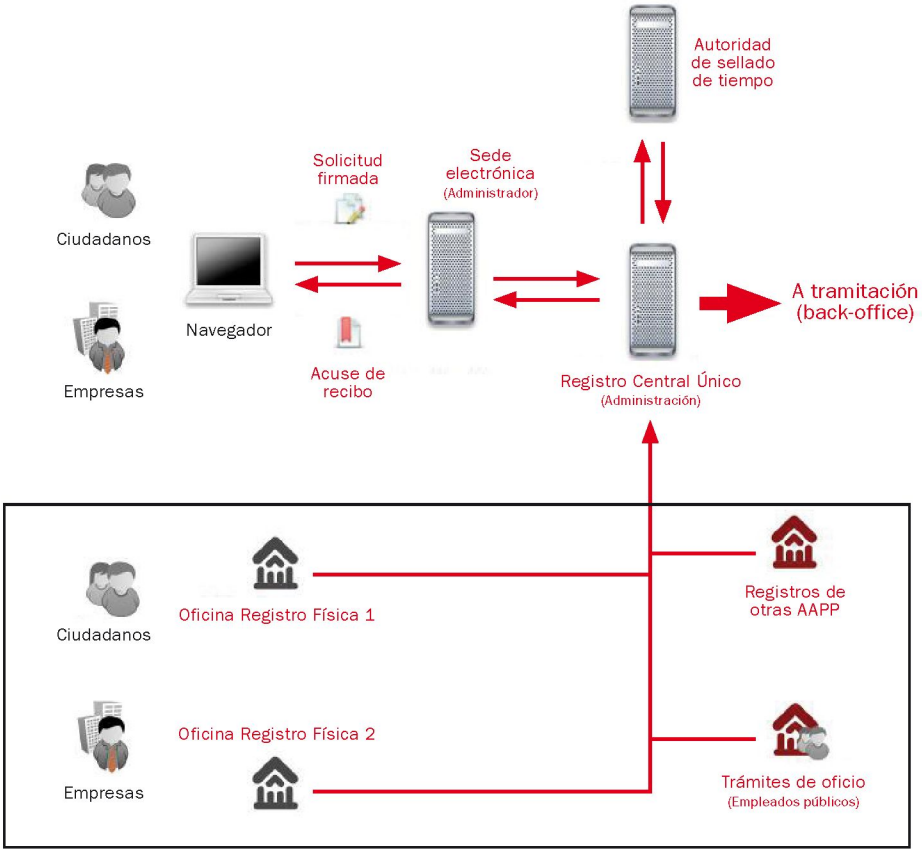


Fig.27

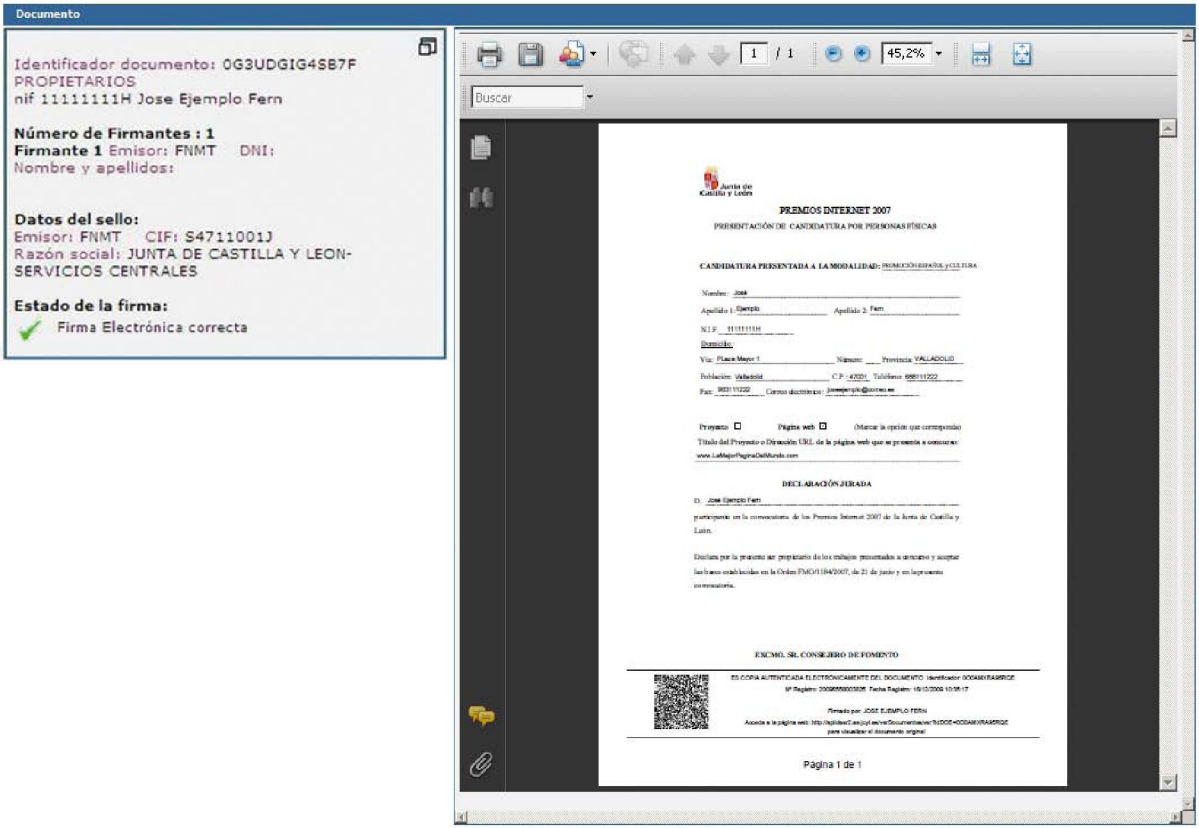
Diagrama funcional del registro electrónico por el CENATIC[10]

10. www.cenatic.es/laecsp/page7/page8/page8.html

Las Administraciones que procedan a la implementación de un registro electrónico tendrán que tener en cuenta una serie de requisitos que aparecen reflejados en los artículos 24, 25 y 26 de la LAECSP. De ellos, es necesario destacar el que aparece en el art. 25.3, por el que se establece que *"los registros electrónicos emitirán automáticamente* ***un recibo*** *consistente en* ***una copia autenticada del escrito****, solicitud o comunicación de que se trate, incluyendo la* ***fecha y hora de presentación y el número de entrada de registro***". Como ejemplo, en la siguiente figura aparece el recibo emitido por el registro electrónico puesto en marcha desde la Junta de Castilla y León.

Fig.28

Recibo emitido por el registro electrónico habilitado por la Junta de Castilla y León



Este requisito nos permite determinar las necesidades que, respecto a identificación, tienen que ser satisfechas por todo registro electrónico, tanto desde el punto de vista de la Entidad como desde el punto de vista del ciudadano:

Identificación de la Entidad: bajo las premisas antes descritas, la Entidad inicialmente debe contar con:

- **Los sellos electrónicos** pertinentes que certifiquen la recepción y cumplimenten a la copia electrónica que se pone en disposición del ciudadano.

- **La referencia temporal** que establezca el momento de la recepción del documento (o documentos) y que cumplimentará, junto con el sello electrónico de la Entidad responsable y el número de entrada de registro, el recibo facilitado al ciudadano en el momento de efectuarse el registro. Hay que tener en cuenta que cuando un ciudadano presenta una solicitud, o cualquier otra documentación, es determinante que se establezca el momento en el que ésta se lleva a cabo para el cómputo de plazos. Para establecer esta referencia temporal podemos optar por el uso de un **sello de tiempo** o una **marca temporal**, pero antes de tomar una decisión a este respecto, es interesante que primero analicemos como se han venido llevando a cabo los registros hasta este momento. Cuando un ciudadano llegaba a la oficina de registro de una Entidad, el empleado de la ventanilla le daba una fotocopia de la solicitud presentada con una firma, un sello y una referencia temporal que venía en función de la hora de su reloj o del reloj de la pared. Por lo tanto, si nos regimos por el criterio de proporcionalidad, bastaría con el uso de **marcas temporales** acreditadas por el mismo organismo titular del registro.

Identificación del ciudadano: a la hora de permitir la entrega de una solicitud, comunicación,... es necesario que la entidad de registro se cerciore de que el ciudadano en cuestión sea quien dice ser, y que dicho ciudadano pueda establecer su conformidad con aquello que entrega.

Para ello, es necesario que la persona, **sea de la naturaleza que sea**, cuente con los instrumentos para poder llevar esto a cabo, es decir, debe contar con los **sistemas de identificación y firma electrónica**, **que bajo el principio de proporcionalidad sean necesarios**, y que han sido comentados en el apartado dedicado a la *"identificación de los ciudadanos."*

A pesar de que podríamos pensar que todos los registros tienen las mismas necesidades, y por tanto todas las soluciones de registros iban a solicitar estar en disposición de la misma tipología de sistemas de identificación y firma electrónica, esto no es así. Un ejemplo de esta diversidad la podemos encontrar comparando los requisitos establecidos para dos registros electrónicos reales como son el del Ministerio de Justicia y el de la Junta de Castilla y León.

En la Orden JUS/3000/2009, de 29 de octubre, por la que se crea y regula el Registro Electrónico del Ministerio de Justicia se determina un amplio margen de sistemas:

"a) *Los sistemas de identificación y firma electrónica incorporados al documento nacional de identidad para personas físicas.*

b) *Los sistemas de firma electrónica avanzada y firma electrónica reconocida.*

c) *Las claves concertadas previo registro como usuario, la información conocida por ambas partes u otros sistemas no criptográficos, en los términos que especifiquen las instrucciones de acceso y utilización del Registro Electrónico en cada procedimiento disponible en la sede electrónica del departamento."*

Por su parte, la Orden PAT/136/2005, de 18 de enero, por la que se crea el registro telemático de la Administración de la Comunidad de Castilla y León y se establecen criterios generales para la presentación telemática de escritos, solicitudes y comunicaciones de determinados procedimientos administrativos, insta a los interesados a disponer específicamente del certificado digital de clase 2CA emitido por la Fábrica Nacional de Moneda y Timbre para poder hacer uso del registro electrónico. Este aspecto fue ampliado gracias a la Orden ADM/912/2009, de 13 abril, por la que se modifica la orden PAT/136/2005, y que establecía como necesario el disponer de DNIe, o de un certificado digital de clase 2CA de firma electrónica emitido por la Fábrica Nacional de Moneda y Timbre, así como aquellos otros certificados electrónicos que hubieran sido previamente reconocidos por esta Administración y fuesen compatibles con los diferentes elementos habilitantes y plataformas tecnológicas corporativas.

Teniendo en cuenta estas observaciones, cada Administración Local deberá establecer, en función de su realidad, los sistemas de identificación y firma admisibles en

su registro electrónico, siempre bajo el principio de proporcionalidad, y ofreciendo las suficientes garantías en materia de seguridad e integridad.

Cumplimentando este sistema, debe ponerse en marcha el servicio **de validación de sellos y cotejo de documentos electrónicos**, para que los ciudadanos puedan comprobar que los documentos electrónicos de los que disponen tienen todas las garantías jurídicas.

5.3 COMUNICACIONES ELECTRÓNICAS

En la LAECSP se dedica un extenso art. 27 a lo que denomina *comunicaciones electrónicas*, pero en él no aparece una definición de qué está contenido bajo este concepto. Si nos remitimos al análisis que aparece el libro *"La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos"*, coordinado por Eduardo Gamero Casado y Julián Valero Torrijos, con este término se está englobando a las comunicaciones *"relativas a avisos e incidencias, las de presentación de reclamaciones o quejas, las de la formulación de sugerencias, y otras formas de presentación que carecen de una regulación específica, así como informaciones y avisos mediante SMS que las Administraciones dirijan a los particulares a propósito de la presentación de servicios públicos, e incluso comunicaciones entre diversas Administraciones Públicas o entre distintos órganos administrativos de una misma Administración"*.

Para la implementación de estas comunicaciones electrónicas, como se indica en el anteriormente nombrado art. 27 de la LAECSP, se deberá contar con los medios electrónicos que permitan, entre otros, **una identificación fidedigna del remitente y destinatario**. Para ello, los requisitos de seguridad e integridad se establecerán en función del caso, y acorde al carácter de los datos que son objeto de la comunicación, pero siempre de acuerdo con **criterios de proporcionalidad** y conforme a lo dispuesto en la legislación respecto a la protección de datos. Por lo tanto lo aconsejable es analizar el servicio en concreto, determinar los riesgos conforme al tipo de información con la que trabaje ese servicio, y en función de ello determinar cómo implementarlo, esto incluye determinar los sistemas de identificación a utilizar tanto por parte de la Administración Pública como del ciudadano como usuario.

La interpretación del término *comunicaciones electrónicas* con la que hemos partido no es la única, ya que por ejemplo en la Junta de Castilla y León, bajo este término, se engloban las notificaciones electrónicas fehacientes donde el tiempo no es un dato relevante. De hecho, se hace uso de la misma aplicación para implementar tanto estas *comunicaciones electrónicas* como las notificaciones electrónicas, de manera que igualmente **utilizan los mismos sistemas de identificación en ambos casos**. Estos últimos serán explicados más extensamente en el apartado dedicado a *"notificaciones electrónicas"*.

En la imagen que aparece a continuación, aparece el buzón electrónico para el ciudadano habilitado por la Junta de Castilla y León para la recepción de notificaciones y comunicaciones electrónicas.

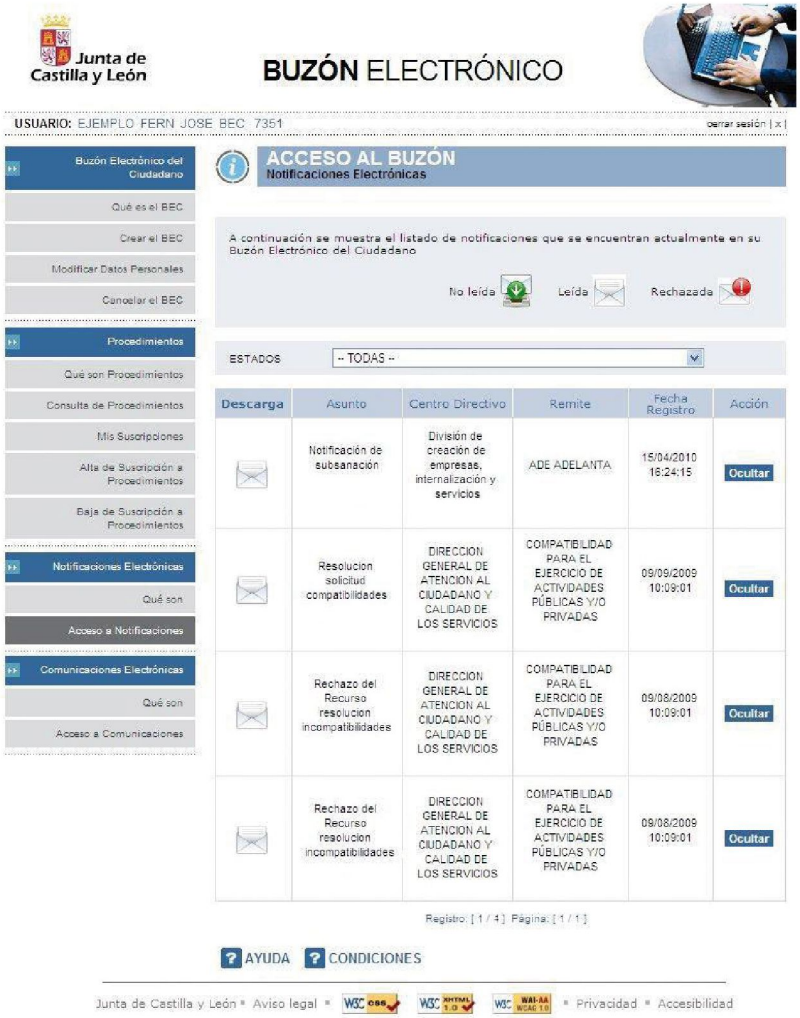


Fig.29

Buzón electrónico del ciudadano habilitado por la Junta de Castilla y León

5.4 NOTIFICACIÓN ELECTRÓNICA

Cuando una Administración Pública tiene que comunicar a un ciudadano el resultado de una resolución o acto administrativo que afecte a sus derechos e intereses hace uso de las notificaciones, como aparece reflejado en el art. 58 de la Ley 30/1992. Además, y dentro de esta misma Ley, en su art. 59, se contempla que las notificaciones **se pueden realizar por cualquier medio que permita tener constancia de la recepción por el interesado o su representante**, **así como de la fecha**, **la identidad y el contenido del acto notificado**.

En este sentido, la LAECSP, en su art. 28, impulsa de manera definitiva el desarrollo e implantación de sistemas que permitan habilitar el canal telemático para el envío de este tipo de comunicaciones. Hay que destacar la importante contribución del uso de las notificaciones electrónicas como nuevo instrumento de comunicación entre ciudadano y Administración, ya que contribuyen tanto a simplificar esta relación, como a la optimización de los recursos (tiempo, dinero, papel) para llevarlas a cabo.

La LAECSP determina los requisitos mínimos que un sistema de notificaciones debe cumplir, apoyándose en las consideraciones definidas en la Ley 30/1992, ya que a fin de cuentas, independientemente del medio utilizado, el ciudadano tiene que contar con las mismas garantías:

- El interesado **deberá señalar el medio electrónico como preferente**, y podrá requerir en cualquier momento que las notificaciones sucesivas no se practiquen por ese medio (art. 28.1 de la LAECSP).

- Deberá permitir acreditar la **fecha y hora** en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso al contenido, para el cómputo de plazos (art. 28.2 de la LAECSP).

- Tras diez días naturales sin que se acceda al contenido, tras la puesta a disposición del interesado, la notificación se considera rechazada (art. 28.3 de la LAECSP).

- Producirá los efectos propios de la notificación por comparecencia, el acceso

electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dicho acceso (art. 28.4 de la LAECSP).

Para dejar constancia de la recepción de la notificación por el interesado, que como ya se comentó aparece recogida en el art. 59 de la Ley 30/92, y centrándonos en el medio electrónico, se hace necesario estar en disposición de los mecanismos de autenticación que garanticen la exclusividad de uso y la identidad del usuario. Esto queda reflejado de forma expresa en el art. 39 R.D. 1671/2009, sobre la notificación, mediante la puesta a disposición del ciudadano del documento electrónico, a través de una **dirección electrónica habilitada**.

En base a lo dicho, no hay una única manera de llevar a cabo una notificación electrónica, siempre que cumpla con estos requisitos. Entre las opciones más habituales, y que están siendo utilizadas por distintas Administraciones Públicas, nos encontraríamos:

UNA DIRECCIÓN ELECTRÓNICA HABILITADA

Como podemos deducir del título, el ciudadano debe disponer de una dirección electrónica habilitada para recibir las notificaciones electrónicas, como se indica en el art. 2 del Decreto 209/2003 de 21 de febrero por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, por el que se modifica el art. 12 Real Decreto 263/1996, de 16 de febrero, que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la AGE. Según este R.D., esta **dirección electrónica** será de carácter único respecto a todas las posibles notificaciones a practicar por la AGE y sus organismos públicos, de ahí que reciba la denominación de **Dirección Electrónica Única** (DEU). Además, en ese mismo artículo se indica que la **DEU** deberá cumplir los siguientes requisitos:

"• *Poseer identificadores de usuario y claves de acceso para garantizar la exclusividad de su uso.*

- *Contar con mecanismos de autenticación que garanticen la identidad del usuario.*
- *Contener mecanismos de cifrado para proteger la confidencialidad de los datos.*
- *Cualquier otro que se fije legal o reglamentariamente".*

En este mismo artículo también se determina que *"la DEU tendrá vigencia indefinida, excepto en los supuestos en que se solicite su revocación por el titular, por fallecimiento de la persona física o extinción de la personalidad jurídica, que una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de notificaciones, supuesto en el cual se inhabilitará la dirección electrónica única, comunicándoselo así al interesado."*

Con estas premisas ya estamos en disposición de determinar los requerimientos que sobre identificación deberemos contemplar en el sistema de notificaciones que deseemos implementar bajo este modelo.

Por parte de la **Administración**, esta debe disponer de:

- Una sede electrónica plenamente constituida, a través de la cual se tenga acceso a la plataforma que habilita el servicio de notificación electrónica.
- Los sellos de órgano correspondientes que permitan su identificación como emisores de esas notificaciones, ya sea en nombre de un departamento o de un área o de la Entidad como institución, según el caso.
- Utilizar marcas de tiempos[11] o contar con los servicios de una TSA, que se encargue de imponer los sellos de tiempo que permitan tener constancia del momento en que se produce un determinado cambio de estado en una notificación, y así poder llevar acabo correctamente el cómputo de plazos.

Por parte del **usuario**, los requerimientos de identificación van a venir determinados por los requisitos definidos para la DEU:

- Disponer de una DEU, que va a ser puesta a disposición del usuario una vez solicitada.

11. Un ejemplo del uso de la marca de tiempo en este contexto lo encontramos en la Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre, más concretamente en su art. 7.

- Poseer identificadores de usuario y claves de acceso para garantizar la exclusividad de su uso.

- Contar con mecanismos de autenticación que garanticen la identidad del usuario, lo que supone estar en disposición del DNIe o sistemas de firma electrónica avanzada o reconocida.

- Contener mecanismos de cifrado para proteger la confidencialidad de los datos.

Para ayudarnos a comprender los requerimientos, se adjunta el esquema del sistema de notificaciones electrónicas de la Junta de Andalucía de modo ilustrativo.

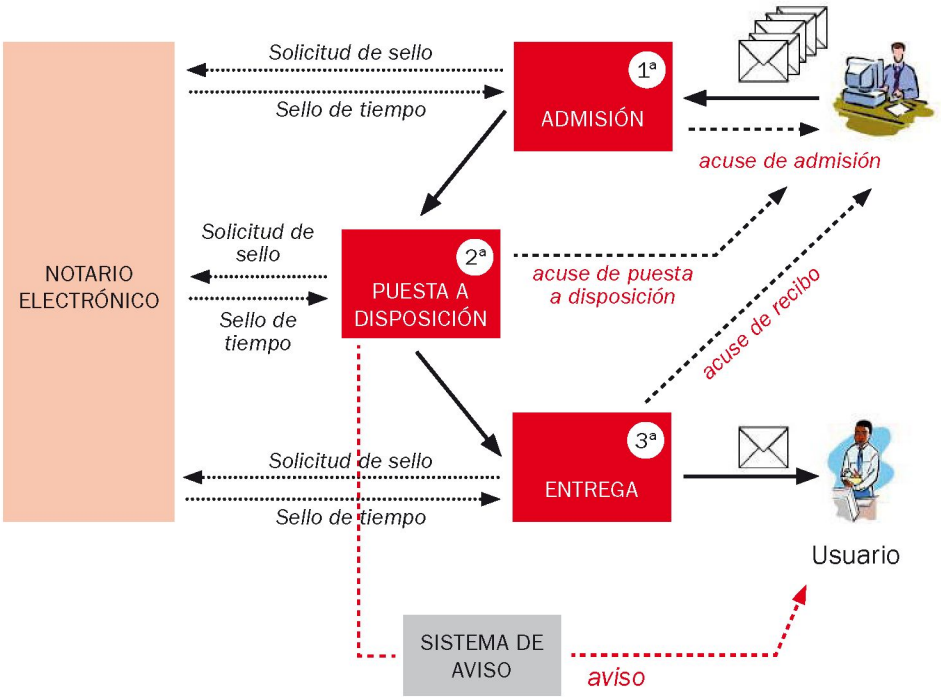


Fig.30

Esquema del sistema de notificaciones electrónicas de la Junta de Andalucía

Si nos detenemos en el esquema, es necesario aclarar dos elementos que pueden resultar confusos:

- El notario electrónico, que se encarga de la generación de un sello de tiempo, de tal modo que es el encargado de hacer constar que un proceso se llevó a cabo correctamente en un momento dado, es decir sería una TSA.

- El sistema de aviso, es un servicio adicional y que no cuenta con valor jurídico, gracias al cual se informa al ciudadano de la recepción de notificaciones (Ej.: un mensaje al móvil informando de la llegada de una notificación a su DEU).

La Junta de Castilla y León dispone de una aplicación propia para la realización de estas notificaciones electrónica, de la que se muestra su apariencia en las siguientes imágenes.

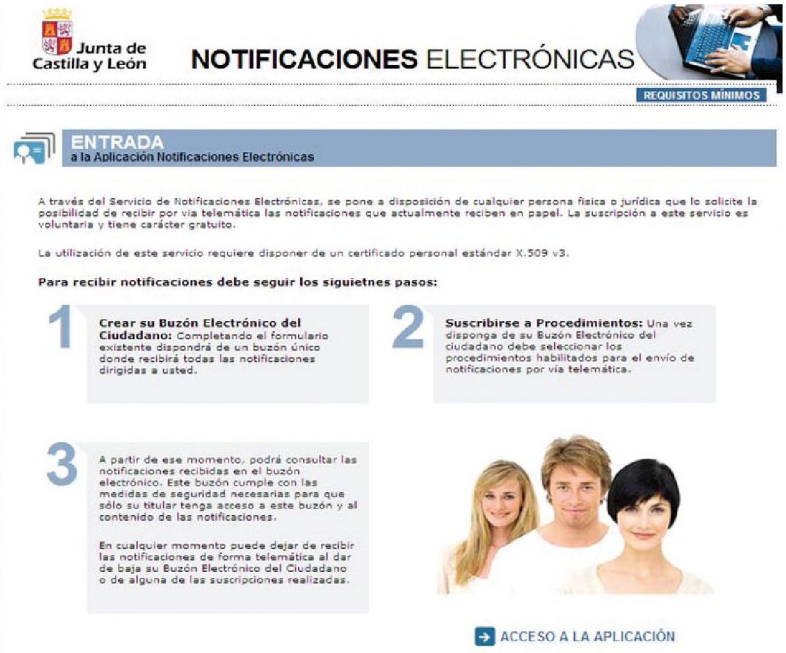
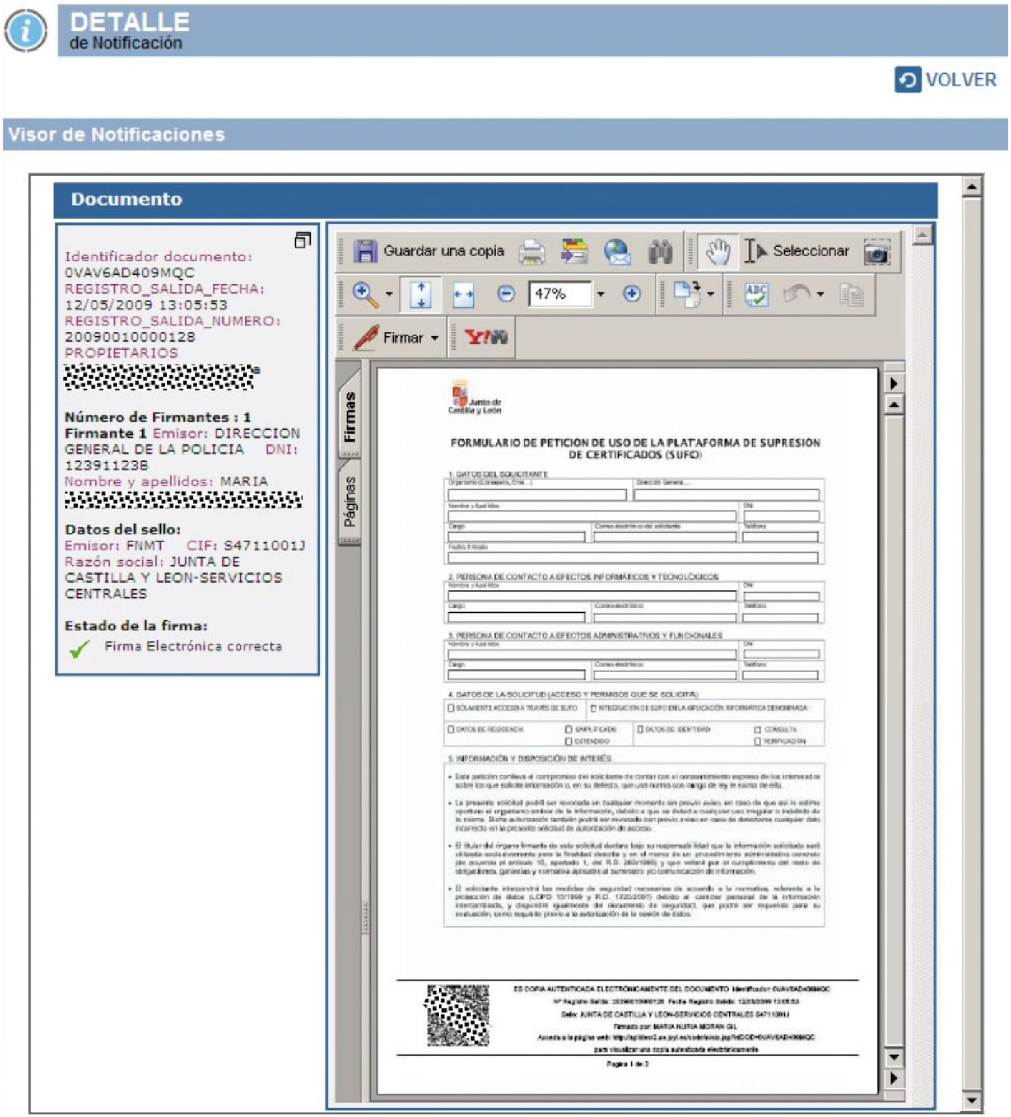


Fig.31

Aplicación para la realización de notificaciones electrónicas puesta en marcha por la Junta de Castilla y León

Fig.32

Detalle de una notificación electrónica a través de la aplicación puesta en marcha por la Junta de Castilla y León



Además, en el art. 39 R.D. 1671/2009, se contempla la posibilidad de que se puedan llevar acabo **notificaciones en las direcciones de correo electrónico que los ciudadanos elijan**, siempre que se genere automáticamente y con independencia de la voluntad del destinatario un acuse de recibo que deje constancia de su recepción y que se origine en el momento de la notificación.

NOTIFICACIÓN POR COMPARECENCIA ELECTRÓNICA

En el art. 40 del R.D. 1671/2009 se determina otra nueva forma de proceder a la notificación, en este caso mediante la fórmula de **notificación por comparecencia electrónica**, que consiste en el acceso del interesado, con la debida acreditación de su identidad, al contenido de la actuación administrativa correspondiente a través de la sede electrónica de la Entidad. Esta opción requiere que:

"a) *Con carácter previo al acceso a su contenido, el interesado deberá visualizar un aviso del carácter de notificación de la actuación administrativa que tendrá dicho acceso.*

b) *El sistema de información correspondiente dejará constancia de dicho acceso con indicación de fecha y hora."*

En este caso, sería necesario que la Entidad que habilite este servicio, ponga a disposición de los ciudadanos una sede electrónica plenamente constituida, con los sistemas de identificación y autenticación que garantice las condiciones de acceso necesarias para garantizar el cumplimiento de los requerimientos anteriormente citados.

Por su parte, los ciudadanos deberán disponer de los sistemas de identificación que sean requeridos (DNIe, sistemas de firma electrónica avanzada o reconocida).

OTROS

Debido a que no está restringida la fórmula para realizar estas notificaciones electrónicas siempre que se respeten los requisitos establecidos por la LAECSP, además de las opciones ya comentadas, existen otras más peculiares entre las que se encuentra el uso de **SMS**.

Como ejemplo de este tipo de implementación, podemos remitirnos al Ayuntamiento de Lleida, que fue pionero en la prestación del servicio de envío de SMSs certificados, y su aplicación en el área de las **notificaciones** frente a terceros. El funcionamiento de este servicio puede resumirse de la siguiente manera:

1. La Administración envía un SMS a través de Internet, haciendo uso del servicio facilitado por la operadora de SMS contratada.

2. El mensaje es enviado al usuario haciendo uso de la red del operador móvil pertinente. Además, el operador móvil, una vez entregado y recibido el mensaje en el móvil del ciudadano indicado, lo notifica a la operadora de SMS.

3. La operadora de SMS genera el acuse de recibo y lo envía a la TSA para añadir el sello de tiempo, obteniendo así un documento firmado y sellado electrónicamente.

4. Finalmente, este acuse de recibo es enviado a la cuenta de correo electrónico del ciudadano.

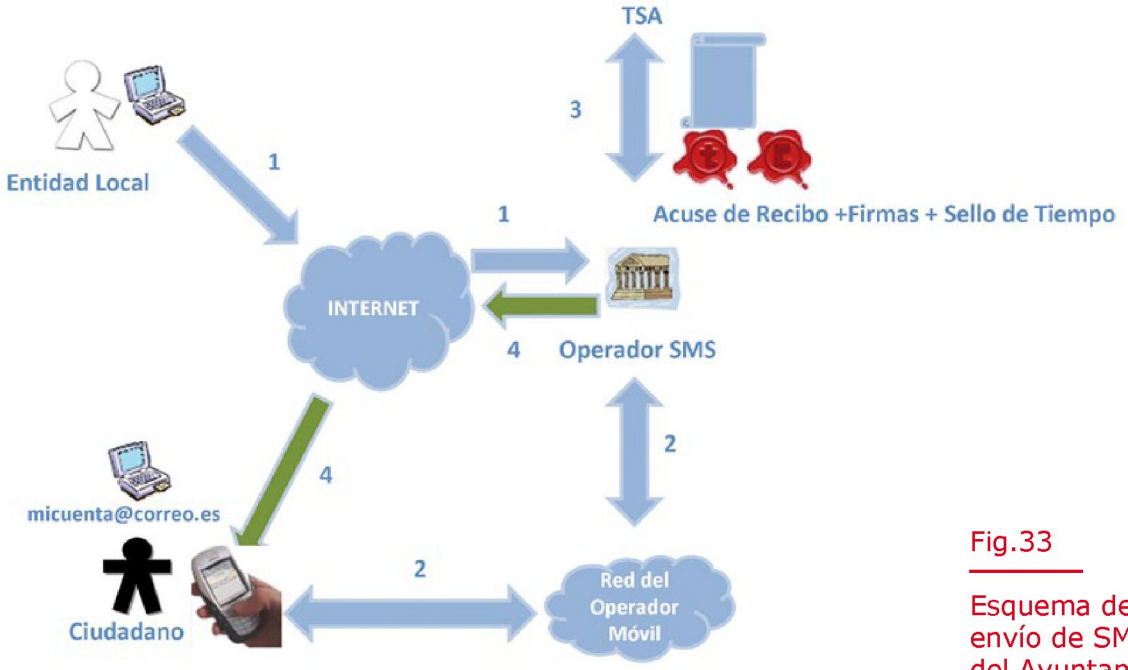


Fig.33

Esquema del servicio de envío de SMSs certificados del Ayuntamiento de Lleida

5.5 PERFIL DE CONTRATANTE

La Ley 30/2007, de 30 de octubre, de Contratos del Sector Público (en adelante LCSP), introduce como novedad para las Administraciones Públicas en su **art. 42 el concepto de perfil de contratante**, *"con el fin de **asegurar la transparencia y el acceso público a la información relativa a su actividad contractual**", para lo cual los órganos de contratación lo "**difundirán, a través de Internet**"*, o lo que es lo mismo, a través de la **sede electrónica** que el organismo tenga habilitada.

Para llevar a cabo esta publicación, y como también se indica en el antes citado art. 42 *"el sistema informático que soporte el perfil de contratante deberá contar con un dispositivo que permita **acreditar fehacientemente el momento de inicio de la difusión pública** de la información que se incluya en el mismo"*.

Así pues, como aparece reflejado en los requisitos determinados en la normativa antes comentada, el tiempo se convierte en un elemento fundamental y crítico. Esto es debido a que todas las actividades y tareas del proceso de contratación han de realizarse en un orden concreto, por ejemplo: la concurrencia de empresas depende de la publicidad de la licitación y la causa de recibir ofertas es la publicidad del anuncio de la licitación.

Pues bien, para lograr dar cumplimiento a los requisitos de fehaciencia que exige la Ley, respecto al momento del inicio de la difusión, será necesario un **sellado de tiempo** de los documentos, que acredite que la publicación de una información en el perfil de contratante, tuvo lugar en un determinado momento y que desde ese momento los datos no han sido modificados, hecho que queda abalado por la TSA.

Teniendo en cuenta las consideraciones jurídicas ya indicadas en el apartado dedicado a "*sellos y marcas de tiempo*", en el caso del perfil de contratante, es aconsejable el empleo de TSAs registradas por el MITYC.

Además, la LCSP también especifica los documentos que se deberán publicar en el perfil de contratante, distinguiendo por su carácter en obligatorios y potestativos. Por tanto, teniendo en cuenta que no toda la información relativa a los procedimientos de contratación tiene porque ser publicada en el perfil de contratante, es una buena práctica dejar constancia y sellar temporalmente toda la información que voluntariamente se inserte en el perfil de contratante, sin distinguir por tanto entre documentación obligatoria y potestativa.

Con respecto a la firma electrónica de los documentos públicos que se publiquen en el perfil de contratante, en el apartado f) de la **disposición adicional decimonovena de la LCSP**, dedicada al uso de los medios electrónicos, informáticos y telemáticos en los procedimientos regulados en esta Ley, se indica que "***todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas que tengan efectos jurídicos*** *y se emitan tanto en la fase preparatoria como en las fases de licitación, adjudicación y ejecución del contrato deben ser autenticados mediante* ***una firma electrónica reconocida*** *de acuerdo con la LFE. Los medios electrónicos, informáticos o telemáticos empleados deben poder garantizar que la firma se ajusta a las disposiciones de esta norma*".

Un buen ejemplo de implementación del perfil de contratante es el que se muestra a continuación, perteneciente al Ayuntamiento de Zaragoza.

Fig.34

Perfil de contratante del Ayuntamiento de Zaragoza

Fig.35

Publicación de un anuncio de licitación en el perfil de contratante del Ayuntamiento de Zaragoza

5.6 DOCUMENTO ELECTRÓNICO

En el anexo de la LAECSP encontramos la definición de documento electrónico, definición que ya ha sido sometida a modificación en el art. 5 LMISI, por la que ha quedado redactada de la siguiente manera: *"se considera **documento electrónico** a la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado"*.

De forma más concreta, en el art. 29 de la LAECSP se encuentran las condiciones específicas de un documento para ser un **documento administrativo electrónico**, en él se determina:

- La validez de los documentos administrativos electrónicos será tal, **siempre que incorporen una o varias firmas electrónicas** de las determinadas para la identificación y autenticación electrónica de las Administraciones Públicas en el ejercicio de su competencia (art. 29.1 de LAECSP).

- Deberán de incorporar **una referencia temporal** cuando así se requiera (art. 29.2 de la LAECSP).

Evidentemente, estas consideraciones son muy generales, debido a que en este apartado se engloba todo documento electrónico en manos de las Administraciones Públicas, de manera que las especificaciones propias de cada tipo de documento se deberán determinar según su naturaleza. Aun así, estas vagas especificaciones ponen de manifiesto la importancia de uno de los grandes grupos de sistemas de identificación que se ha ido desgranando con anterioridad, como es el que se concentra en la **identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia**. Por otro lado, también adquiere relevancia el uso de **los sellos de tiempo o las marcas temporales**, en función de los requerimientos del documento del que se trate.

Para que los documentos incorporen los elementos antes comentados, que permitirán dotarles de las garantías que respecto a identificación, autenticación y referencia temporal necesitan, es preciso que el formato que los soporte pueda almacenarlos. A

este respecto, además también tendrán que tenerse en cuenta una serie de aspectos que aunque no están especificados expresamente en la LAECSP, se pueden inferir de las previsiones legales referentes a la conservación de los documentos electrónicos, la neutralidad tecnológica y uso de estándares (arts. 11 y 23) y de las relacionadas con su recuperación y conservación (art. 21) que podemos encontrar en el ENI.

Un ejemplo sobre la elección y uso de formatos lo podemos encontrar en la implementación del nuevo BOE electrónico. En este caso se usa, **para garantizar su visibilidad**, el formato de documento electrónico administrativo PDF/A-1a, que está espacialmente diseñado para generar documentos accesibles. Este formato permite que por ejemplo una persona con deficiencias visuales pueda utilizar un documento de este tipo ayudándose de un lector de pantalla.

Otros formatos a destacar serían los XAdES/CAdES, con los que se **garantiza la integridad del documento**, y que son útiles para llevar a cabo el archivo electrónico de documentos, pero que son más complejos a la hora de ser utilizados por los ciudadanos. Otro ejemplo de elección de formatos en función del uso la encontramos en la Orden ITC/1475/2006, de 11 de mayo, sobre la utilización del procedimiento electrónico para la compulsa de documentos en el ámbito del Ministerio de Industria, Turismo y Comercio. En ella se hacen consideraciones semejantes a las formuladas en el caso del BOE.

Con esto queremos destacar que es habitual que un documento que se almacene utilizando XAdES/CAdES, pero de cara al ciudadano se presente en formatos más habituales para él, como el formato PDF/A.

5.7 COPIAS ELECTRÓNICAS

Las copias electrónicas ocupan el art. 30 de la LAECSP, y en él se contemplan tres tipos de copias electrónicas en función de las características del original a partir del cual se pretende hacer la copia:

- Copias electrónicas de documentos electrónicos.

- Imágenes electrónicas de documentos en papel.
- Copias en papel de documentos electrónicos.

Como se puede deducir de su propio nombre, las copias en papel de documentos electrónicos no son copias electrónicas, pero son también tratadas en este documento para abarcar todas las posibilidades que surgen debido a la convivencia de los dos formatos en las Administraciones Públicas.

En este apartado vamos a ir tratando cada una de ellas, identificando sus requisitos más significativos.

Además, para poder definir más concretamente los requisitos que sobre identificación y autenticación son necesarios en estos procesos, también hay que contemplar lo expuesto en el R.D. 1671/2009, al que se hará referencia.

Por último, hay que recordar que el proceso de copiado electrónico, al igual que otros aspectos relevantes, estarán contenidos de forma más exhaustiva en el ENI, a través de la fórmula de norma técnica como se indica en su disposición adicional primera.

La Junta de Castilla y León dispone del aplicativo ***Copias Originales Electrónicas***, que es capaz de realizar copias originales desde soporte papel a electrónico y viceversa, así como de soporte electrónico a electrónico, abarcando por tanto todo el abanico de posibilidades. A continuación se muestra la pantalla de presentación del aplicativo, en la que aparecen claramente los botones de acceso a las dos funcionalidades que implementa:

- Realizar copia de documento en papel: para la realización de copias de documento en papel a documentos electrónicos, y su posterior almacenamiento.
- Realizar copia de documento electrónico: con la que se podrá obtener copias originales en formato electrónico o en papel de documentos previamente almacenados.

Fig.36

Pantalla de presentación del aplicativo Copias Originales Electrónicas de la Junta de Castilla y León

COPIAS ELECTRÓNICAS DE DOCUMENTOS ELECTRÓNICOS

La LAECSP, en su art. 30, prevé la posibilidad de realizar copias electrónicas de documentos electrónicos **con plena validez jurídica** siempre que se cumpla lo indicado en el art. 46 de la Ley 30/92, en el que se indica que:

"1. *Cada Administración Pública determinará reglamentariamente los órganos que tengan atribuidas las competencias de expedición de copias auténticas de documentos públicos o privados.*

2. *Las copias de cualesquiera documentos públicos gozarán de la misma validez y eficacia que estos siempre que exista constancia de que sean auténticas.*

3. *Las copias de documentos privados tendrán validez y eficacia, exclusivamente en el ámbito de la actividad de las Administraciones Públicas, siempre que su autenticidad haya sido comprobada.*

4. *Tienen la consideración de documento público administrativo los documentos válidamente emitidos por los órganos de las Administraciones Públicas."*

Y siempre que:

- El documento original esté en poder de la Administración.
- La información de la firma electrónica o en su caso el sellado de tiempo permita comprobar la coincidencia entre original y copia.

Este último requisito exige que en la sede electrónica de la Entidad, se cuente con las aplicaciones que hagan posible esa comprobación.

Para proceder a tratar este tipo de copias electrónicas, es necesario realizar otra categorización en función de si se producen cambios de formato en el proceso de copia.

Por lo tanto podemos encontrarnos:

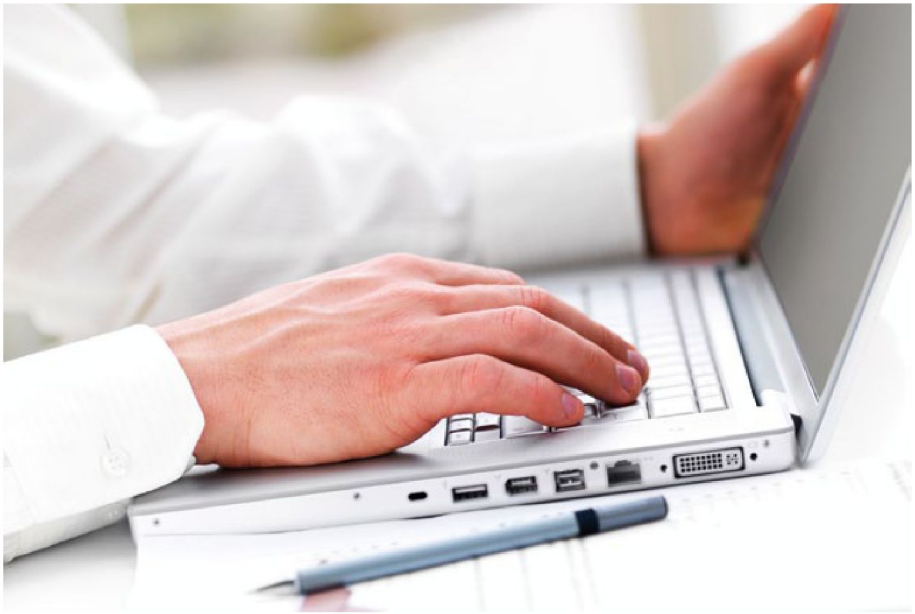
- **Copias electrónicas de documentos electrónicos sin cambio de formato**: En este caso, y remitiéndonos al art. 43 del R.D. 1671/2009, *"las copias electrónicas así generadas, por ser idénticas al documento electrónico original tanto en formato como en contenido, tendrán la eficacia jurídica de documento electrónico original"*. Debemos por tanto entender, que son copias electrónicas obtenidas por un proceso directo de copia.

- **Copias electrónicas de documentos electrónicos con cambio de formato**: en este caso deberán de cumplir una serie de requisitos adicionales, como también queda recogido en el al art. 43 del R.D. 1671/2009:

  *"c) Que incluya su carácter de copia entre los **metadatos asociados**.*

  *d) Que **sea autorizada mediante firma electrónica** conforme a los sistemas recogidos en los artículos 18 y 19 de la LAECSP, de 22 de junio."*

Además en el art. 43 del R.D. 1671/2009, se hace una consideración particular sobre la copia electrónica de documentos electrónicos presentados conforme a sistemas normalizados o formularios, ya que además de considerarse como copia auténtica la que cumplan con las condiciones anteriores, se considerará también como auténtica *"el documento electrónico, autenticado con la firma electrónica del órgano u organismo destinatario, resultado de integrar el contenido variable firmado y remitido por el ciudadano en el formulario correspondiente empleado en la presentación"*.



IMÁGENES ELECTRÓNICAS DE DOCUMENTOS EN PAPEL

En esta categoría estarían recogidas tanto las imágenes electrónicas de documentos en papel emitidos por las Administraciones Públicas, como las imágenes electrónicas de documentos privados aportados por los ciudadanos, y que aparecen recogidas en los apartados 2 y 3 del art. 30 de la LAECSP respectivamente.

En el caso de que el original en papel fuese emitido por las Administraciones Públicas, para que la copia sea auténtica tiene que cumplir con lo indicado en el art. 46 de la Ley 30/92, ya comentado.

Por otro lado, cuando los documentos son aportados por los ciudadanos, en el art. 30 de la LAECSP, se indica que las Administraciones Públicas podrán obtener las imágenes electrónicas de estos, con la misma validez y eficacia, a través de procesos

de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia.

Para entender mejor a que se refiere con ***imagen electrónica***, podemos recurrir al art. 44 del R.D. 1671/2009, en el que se define como "***el resultado de aplicar un proceso de digitalización a un documento en soporte papel o en otro soporte que permita la obtención fiel de dicha imagen***". Además, también en ese mismo artículo se aclara que como ***digitalización*** se refiere "***al proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra, del documento***".

En el art. 44 del R.D. 1671/2009, también se especifican los requisitos a cumplir por una Administración para que las copias realizadas en ambos casos sean consideradas auténticas:

"a) *Que el documento copiado sea un original o una copia auténtica.*

b) *Que la copia electrónica* ***sea autorizada mediante firma electrónica*** *utilizando los sistemas recogidos en los artículos 18 (sistemas de firma electrónica para la actuación administrativa automatizada) y 19 (firma electrónica del personal al servicio de la Administración Pública) de la LAECSP.*

c) *Que las imágenes electrónicas estén codificadas conforme a alguno de los formatos y con los niveles de calidad y condiciones técnicas especificados en el ENI*[12]*.*

d) *Que la copia electrónica* ***incluya su carácter de copia*** *entre los metadatos asociados.*

e) *Que la copia sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben."*

Además, y atendiendo al gran volumen de documentación que la Administración va a tener que tratar, en el art. 30 de la LAECSP también se contempla la posibilidad de hacer copias a través de **un proceso automatizado**, para lo que se indica que es necesario el correspondiente **sello electrónico**.

12. En el art. 24 del ENI se indica que *"la digitalización de documentos en soporte papel por parte de las Administraciones públicas se realizará de acuerdo con lo indicado en la norma técnica de interoperabilidad correspondiente en relación con los siguientes aspectos:*
a) Formatos estándares de uso común para la digitalización de documentos en soporte papel y técnica de compresión empleada, de acuerdo con lo previsto en el artículo 11.
b) Nivel de resolución.
c) Garantía de imagen fiel e íntegra.
d) Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización."

A continuación se muestra el acuse de recibo emitido por el aplicativo *Copias Originales Electrónicas* de la Junta de Castilla y León tras la obtención de una copia electrónica a partir de un original en papel.

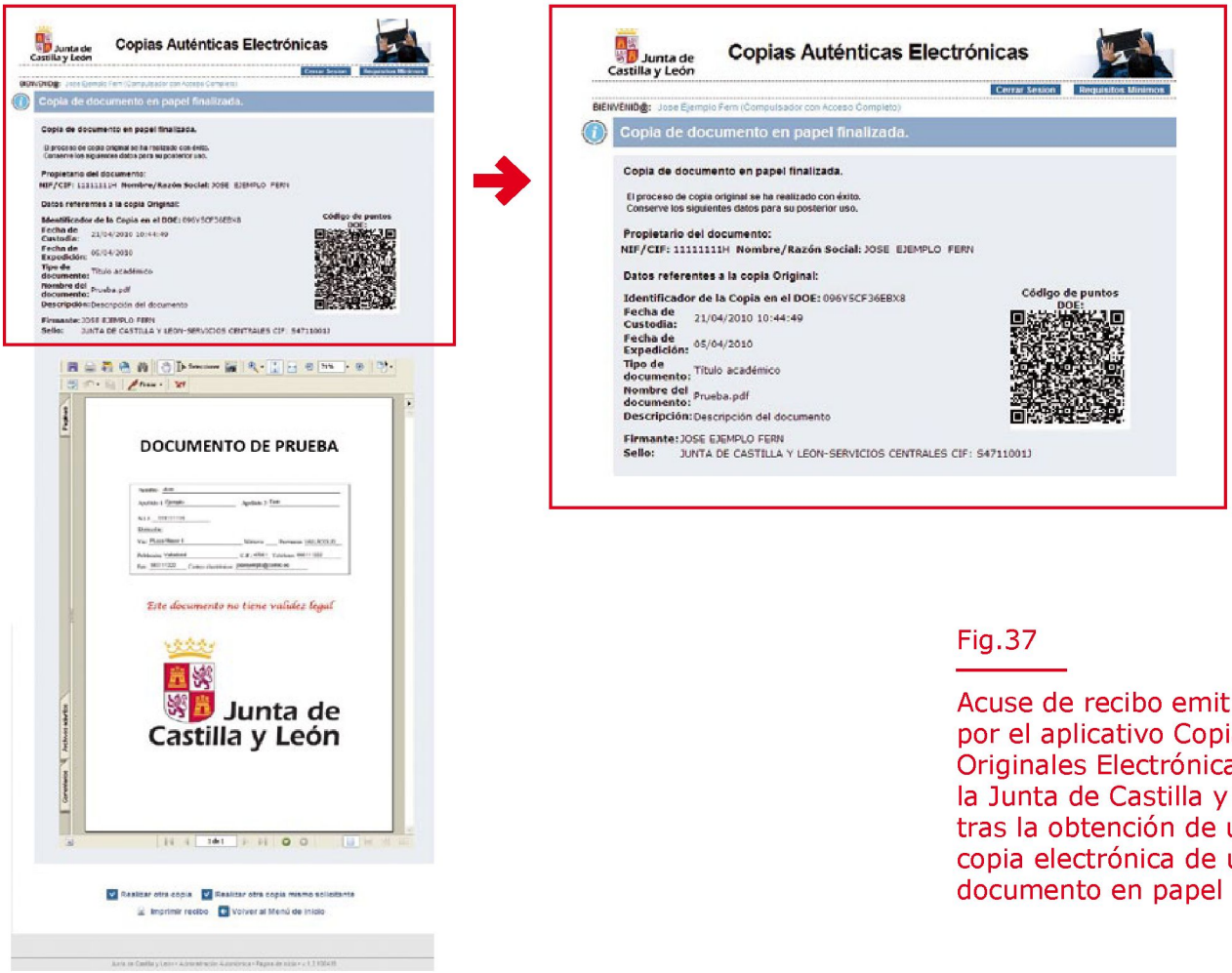


Fig.37

Acuse de recibo emitido por el aplicativo Copias Originales Electrónicas de la Junta de Castilla y León tras la obtención de una copia electrónica de un documento en papel

COPIAS EN PAPEL DE LOS DOCUMENTOS ELECTRÓNICOS

Respecto a este tipo de copias, en la LAECSP únicamente se indica, en su art. 30, que tendrán la consideración de copias auténticas *"siempre **que incluyan** la impresión de un **código generado electrónicamente** u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora"*. Con ello lo que se pretende es evitar la pérdida por su paso al papel de los sistemas de autenticación e identificación incluidos en el documento electrónico original, de manera que se hace necesario que el ciudadano pueda acceder al documento electrónico para las comprobaciones y verificaciones que sean pertinentes.

Además en el art. 45 del R.D. 1671/2009, se amplía la especificación de requisitos a cumplir, e indica que también es necesario que:

"a) Que el documento electrónico copiado sea un documento original o una copia electrónica auténtica."

"c) Que la copia sea obtenida conforme a las normas de competencia y procedimiento, que en cada caso se aprueben, incluidas las de obtención automatizada."

El proceso llevado a cabo para la generación de esas copias electrónicas a partir del original en papel, podemos encontrarlo especificado por ejemplo en la Ordenanza reguladora del procedimiento y la aplicación informática para la producción de copias electrónicas auténticas mediante procedimientos de digitalización y autenticación seguros, publicada el 18 de marzo de 2009 perteneciente al Ajuntament de Sant Boi de Llobregat. En esta ordenanza se estiman los pasos a seguir en el proceso de generación de la copia y las necesidades que en cuanto a identificación y autenticación se requieren:

- **Fase de preparación de los documentos**

  Esta fase consiste en el **estudio y tratamiento de los documentos** para asegurar que se obtendrá de ellos una imagen íntegra y fidedigna en relación al original en papel, para así adecuar el hardware de digitalización a sus características.

También en esta fase se procede a organizar los documentos a escanear, para lo que se requiere que cada expediente y/o documento tiene que **incorporar el número de expediente y/o documento normalizado**.

Fase de captura, digitalización y autenticación de las imágenes

En él se distinguen dos tipos de procedimientos, el individualizado y el automatizado.

- **Procedimiento individualizado**: por el cual los operadores **escanearán el documento en soporte papel** y se guardará el resultado en una imagen electrónica. La imagen electrónica se incluirá en un documento electrónico cuyo formato garantice la larga conservación y la integridad del documento, para su almacenaje en un repositorio provisional de documentos electrónicos. Una vez obtenida la imagen, el empleado público la contrasta con el original para controlar su calidad y detectar posibles defectos de lectura y proceso. Si la copia electrónica es idéntica al documento en papel y la calidad es correcta, se procederá a la autenticación de la imagen electrónica con la **firma electrónica reconocida del funcionario o empleado público, junto con la información de la fecha y hora de la firma y la identificación del firmante**.

- **Procedimiento automatizado**: por el cual los operadores escanearán los documentos en soporte papel para obtener una imagen electrónica, a la que se adjuntará **una firma electrónica consistente en un certificado digital de aplicación**.

  El proceso se realiza mediante una aplicación informática compuesta de diferentes módulos, que son descritos en la propia Ordenanza, cada uno de los cuales estará firmado digitalmente para evitar su manipulación y asegurar la relación entre el código fuente y los propios módulos. Como en el caso anterior, una vez obtenidas las imágenes, y antes de ser grabadas, el operador realizará un control de calidad mediante la visualización de las imágenes. Hay que tener en cuenta que todo este proceso deberá estar debidamente documentado, dejando constancia, en lo que denomina pista de auditoría de las transacciones y trazas realizadas en la propia imagen, que acompañará a cada imagen. Entre esa información se encuentra, por ejemplo, la constancia de la validación del

certificado digital de la aplicación que acompaña a la imagen, la descripción de los metadatos de identificación o la firma y autenticación de las imágenes.

Finalmente tendrán que autenticarse estas imágenes mediante el sello de órgano y de tiempo para poder garantizar su autenticidad, originalidad, integridad y accesibilidad.

- **Fase de archivo**

  En esta última fase, los documentos digitalizados y autenticados se incorporarán al repositorio seguro de documentos electrónicos que debe garantizar, en todo caso, el acceso a la información, y la integridad y autenticidad de los documentos.

En la Junta de Castilla y León, estas copias se realizan a partir de documentos previamente almacenados, haciendo uso del aplicativo *Copias Originales Electrónicas*. Además de permitir hacer copias electrónicas de documentos electrónicas, permite pasar esas copias a papel a través del icono que aparece destacado en la siguiente imagen.

Como se puede ver en la imagen, además de la visualización del documento, se muestra información sobre el propietario del documento, el firmante, los sellos que tenga incorporados y el estado de todas las firmas que lleva.

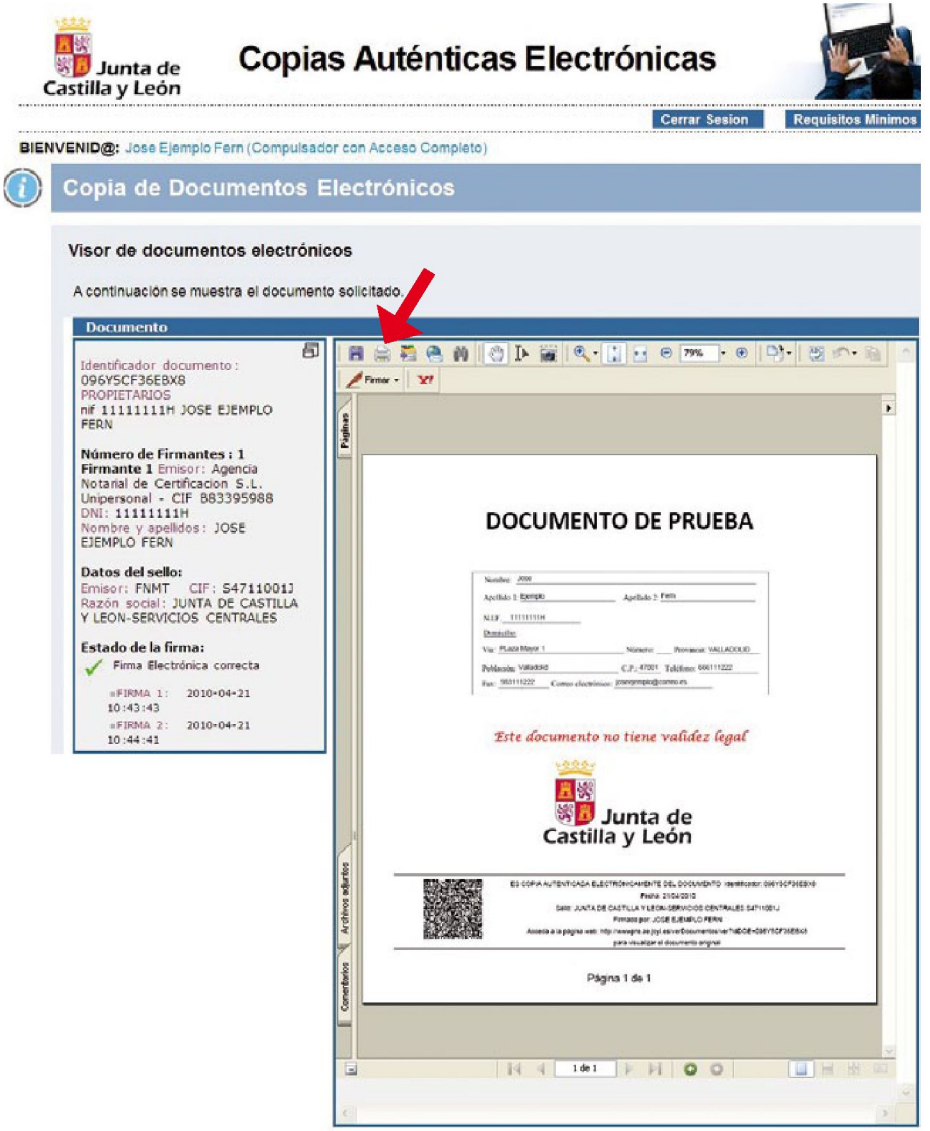


Fig.38

Visor del aplicativo Copias Originales Electrónicas de la Junta de Castilla y León para la obtención de una copia electrónica o en papel de un documento electrónico

5.8 COMPULSA ELECTRÓNICA

La compulsa electrónica no aparece de forma específica en la LAECSP, pero podemos remitirnos a la Orden ITC/1475//2006, de 11 de mayo, sobre la utilización del procedimiento electrónico para la compulsa de documentos en el ámbito del Ministerio de Industria, Turismo y Comercio, en la cual se define concretamente a las compulsas electrónicas dentro del ámbito de actuación de este Ministerio, como *"**un procedimiento seguro de digitalización de la documentación de originales en papel que produce una copia electrónica del documento original**, **utilizando para ello la firma electrónica reconocida de un funcionario o empleado público** del Ministerio o de alguno de sus organismo públicos dependientes, que es la que **garantiza la identidad de los contenidos del documento original y de la copia electrónica**"*.

Por lo tanto, a la hora de establecer los requisitos que las compulsas electrónicas requieren, podemos remitirnos a las consideraciones que la LAECSP hace en los apartados 2 y 3 de su art. 30, en los que se habla de las imágenes electrónicas de documentos en papel emitidos por las Administraciones Públicas y las de documentos privados aportados por los ciudadanos, y que han sido tratados en el apartado anterior bajo el título de *"**imágenes electrónicas de documentos en papel**"*, añadiéndole el matiz de utilizar **la firma electrónica reconocida de un funcionario o empleado público**.

En esta Orden también se especifica, en su art. 2, el procedimiento para llevar a cabo la compulsa distinguiendo los siguientes pasos:

1. Digitalización de los documentos originales en papel a compulsar, produciendo un fichero en formato PDF que se mostrará en la pantalla del ordenador con la imagen obtenida.

2. Cotejo de la imagen del documento original en papel con el mostrado en la pantalla del ordenador.

3. Firma de la copia electrónica mediante la utilización de **firma electrónica reconocida del funcionario o empleado público** que realiza la compulsa, lo que garantiza la identidad de los contenidos del documento original y de la copia.

4. A la copia compulsada se le añadirá **un localizador universal del documento**, así como **la fecha y hora de la compulsa** y la identificación del firmante.

5. Devolución de los originales a los interesados o a los que los presentaron.

La extrapolación de esta norma, a nuestra Entidad Local puede ayudarnos a entender las necesidades que sobre identificación vamos a tener que implementar, y que quedarían concretadas en:

- Que los empleados públicos autorizados para realizar compulsas dispongan de un sistema de firma electrónica reconocida de empleado al servicio de las Administraciones Públicas, o de los sistemas contenidos en el DNIe.

- Se deberá incluir la referencia temporal para asegurar el momento en el que se ha realizado la compulsa. Para ello se deberá acompañar a la compulsa electrónica de una marca de tiempo o de un sello de tiempo, en función de los requisitos que se deban cumplir a este respecto. En general bastará con una marca de tiempo para acreditar esa referencia temporal.

- Localizador universal del documento, que es un requisito indispensable para todo documento electrónico.

El aplicativo de *Copias Originales Electrónicas* de la Junta de Castilla y León, comentado en el apartado dedicado a las *"copias electrónicas"*, posibilita también la realización de compulsas de documentos en papel a documentos electrónicos, y desde documentos electrónicos, obtener documentos compulsados en papel.

5.9 ARCHIVO ELECTRÓNICO

La LAECSP supone el respaldo definitivo al archivo electrónico, como herramienta para almacenar los documentos originados o convertidos a soporte electrónico en el quehacer diario de la Administración. Este hecho queda reflejado en el art. 31.1, en el que se indica que *"podrán almacenarse por medios electrónicos*

todos los documentos utilizados en las actuaciones administrativas".

Otro aspecto a destacar, son las consideraciones que sobre el formato encontramos en art. 31.2 de esta misma Ley, en el que se refleja la necesidad de que los documentos electrónicos hagan uso de formatos que permitan asegurar la identidad e integridad de la información necesaria para reproducirlos, así como asegurar la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. Por otro lado, en el art. 31.3, se determina que *"los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán* ***la identificación de los usuarios y el control de accesos****, así como el cumplimiento de las garantías previstas en la legislación de protección de datos".*

Por lo tanto, las consideraciones de archivado de documentos afectan tanto a la propia creación del documento electrónico, como a la herramienta para soportar el archivo en sí mismo.

Si nos remitimos al ENI, según su art. 21 y en línea con lo anterior, se determina que se deberán tomar una serie de medidas para garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida, de las cuales hay que destacar las siguientes:

"g) *El acceso completo e inmediato a los documentos* ***a través de métodos de consulta en línea*** *que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión a papel de aquellos documentos que sean necesarios. El sistema que se implemente permitirá la consulta durante todo el período de* **conservación al menos de la firma electrónica***, incluido, en su caso,* ***el sello de tiempo****, y de los metadatos asociados al documento.*

h) *La adopción de medidas para* ***asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida****,.. de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo,*

se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de las Administraciones Públicas".

Por lo tanto, acerca del archivo electrónico, además de las consideraciones sobre acceso a la documentación, firma, sellado de tiempo, etc. que están tratadas en otros apartados específicos de este documento, hay que resaltar su aspecto más característico, el hecho de que **los documentos deben conservarse durante un periodo largo de tiempo**. Hay que tener en cuenta, que cuando se firma un documento, no basta con saber que en el momento de la firma ésta es válida, sino que si por ejemplo deseo consultar dentro de 10 años este mismo documento, tengo que poder seguir corroborando que sigue siendo válida.

Para conseguir estos propósitos, y como queda de manifiesto en el art. 22 del ENI, para la conservación del documento electrónico se establece el uso **de formatos de firma longeva** (o de larga duración) que preserven la conservación de las firmas a lo largo del tiempo. Esta firma longeva implica la incorporación a la firma electrónica de los elementos de tiempo y validación que permitan verificar la firma sin necesidad de elementos externos, guardando además todas las evidencias que posibiliten su verificación posterior, e incorporando al archivo de firma todo lo necesario para certificar su validez, es decir crear una firma *completa y autoverificable*. Para ello, existen diferentes versiones para los principales formato de firma existentes (XML DSig /CMS) denominados AdES (Advanced Electrónic Signature) que amplían las capacidades de la firma electrónica y consiguen su longevidad:

- AdES – BES, sería la firma electrónica avanzada.
- AdES – EPES (Explicit Policy Electronic Signature), que emplea políticas de firma.
- AdES – T (Timestamp), en la que se añade un sellado de tiempo, para establecer el momento en el que se ha firmado un documento.
- AdES – C (complete), que añade referencias a los certificados de la cadena de certificación y su estado.

- AdES – X (extended), que añade sellos de tiempo a las referencias introducidas por las AdES – C.

- AdES – XL, que añade los certificados y la información de revocación de éstos. En este caso, se incorpora un sello de tiempo que afecta no sólo a la firma sino también a las referencias a la información de validación, así como la propia información de validación (cadena de certificados y respuesta de revocación).

- AdES – A, que permite seguir añadiendo sellos de tiempo periódicamente para garantizar la integridad de la firma.

Por lo tanto, dentro de todos los tipos aquí expuestos, sería el AdES – XL el que nos permitiría conseguir una firma *autocontenida y autoverificable*.

Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en su política de gestión de documentos. Para ello, además de que los documentos se presenten en los formatos anteriores, en el momento que van a ser revocados, debido a su fecha de validez, se les aplica un nuevo sello temporal que les permite seguir siendo válidos por el periodo de validez de este sello.

Para entenderlo mejor podemos remitirnos a una de las ponencias de las Jornadas de Firma Electrónica organizadas por CatCert el 13 de noviembre 2009, e impartida por Joan Mir, en la que describe cómo solucionar la problemática de la longevidad de las firmas. En ella se indica que las firmas electrónicas simples (CMS/XMLdsig) se pueden conservar válidas durante un periodo, generalmente entorno a los 2 años.

Fig.39

Validez de las firmas electrónicas simples

Los formatos de firma electrónicas avanzadas (-AdES) que disponen de sellos de tiempo, permiten que podamos verificar la validez de los datos firmados en función de ese sello de tiempo, de manera que mientras ese sello sea válido, los datos que están firmados también lo serán.

Fig.40

Validez de las firmas electrónicas avanzadas

Según la LFE, la validez de las firmas electrónicas no podrá ser superior a 4 años, de manera que es necesario implementar un procedimiento por el que se mantenga la validez de estas firmas. Para ello se completa la firma electrónicas avanzadas con sellos temporales, de manera que en el momento en el que se va a caducar la firma se le aplica un sello de tiempo que confirma su validez por un nuevo periodo de tiempo, el periodo de tiempo de vigencia del propio sello. Por tanto, este proceso se repetirá cada cierto tiempo, para sigan siendo válidos.

Fig.41

Solución a la problemática de la longevidad de las firmas electrónicas

El archivo electrónico, al igual que otros aspectos relevantes, estarán contenidos de forma exhaustiva en el ENI, mediante la fórmula de norma técnica, como se indica en su disposición adicional primera.

En la Junta de Castilla y León, el archivo electrónico se lleva a cabo a través de una aplicación denominada ***Depósito de Originales Electrónicos*** (DOE), que es el encargado de custodiar los documentos electrónicos, garantizando su seguridad física y lógica, y su pervivencia en el tiempo. Esta última se consigue gracias a los resellados

que realiza la plataforma que lo implementa, gracias a lo cual es posible garantizar las firmas a lo largo del tiempo. En este caso, el formato de firma que se utiliza es el XAdes antes comentado.

En la siguiente imagen aparece la arquitectura del DOE, donde los tres elementos que lo componen son accesibles mediante servicios web seguros:

- La plataforma de custodia adquirida, que aparece denominada como SIAVAL, consta de:
  - Un sistema de almacenamiento.
  - Una base de datos de gestión.
  - Un servidor web.
- El repositorio de metadatos, que es una base de datos para la gestión de los metadatos de los documentos.
- Las malaquías, que permiten el control de acceso de ciudadanos o empleados públicos a los documentos.

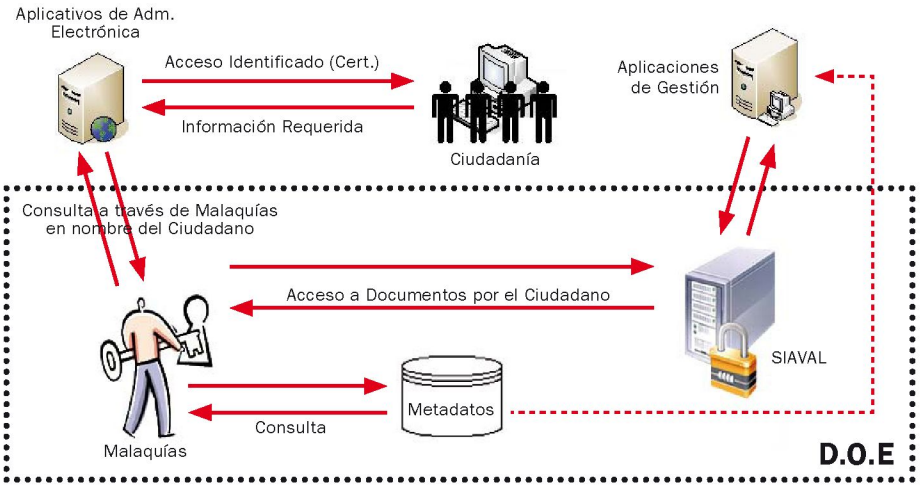


Fig.42

Arquitectura del DOE

5.10 EXPEDIENTE ELECTRÓNICO

El expediente electrónico es la traducción al entorno digital del expediente que hasta ahora se disponía para cualquier procedimiento. Para una definición más formal, podemos dirigirnos al art. 32 de LAECSP, donde se describe *"el expediente electrónico como el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan"*. Este expediente estará caracterizado por un **índice electrónico** para su foliado, **firmado por la Entidad Pública** que proceda.

El índice del expediente en el ENI viene definido como la *"relación de documentos electrónicos de un expediente electrónico"*. Gracias a este índice se *"garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos"* (art. 32 de la LAECSP). Los métodos para salvaguardar esta integridad deberán ser demostrables y fiables, de ahí que se opte por firmar dichos índices.

Dentro del art. 53 del R.D. 1671/2009, y teniendo en cuenta que se desarrolla en el ámbito de la AGE, se indica de forma más específica ciertos aspectos del expediente electrónico que podemos extrapolar a cualquier Administración como:

- La formación del expediente electrónico **es responsabilidad del órgano** que disponga la normativa de organización específica y, **de no existir previsión normativa**, **del encargado de su tramitación**.

- Se incluirá al expediente un **código que permita su identificación** unívoca por cualquier órgano de la Administración en un entorno de intercambio interadministrativo. Este código no aparece especificado en la LAECSP.

- Para el foliado se determina el uso del **índice electrónico**, **firmado electrónicamente** mediante los sistemas de firma electrónica para la actuación administrativa automatizada y del personal al servicio de las Administraciones Públicas.

- Se remite al ENI, a la hora de definir su estructura, formato, especificaciones de los servicios de remisión y puesta a disposición. En este mismo sentido, los documentos electrónicos que contengan **se ajustarán al formato o formatos de larga duración** que también se definen en el ENI a través de su correspondiente norma técnica.

Al igual que en el ámbito de la AGE, el resto de Administraciones Públicas de cualquier nivel, tendrán que atender a las especificaciones que sobre el expediente electrónico se determinan en el ENI. En este caso, y como determina la disposición adicional primera, estas especificaciones se encontrarán en la norma técnica desarrollada al respecto, y en la que se tratará la estructura y formato del expediente electrónico, así como de los requisitos de los servicios de remisión y puesta a disposición.

Por otro lado, y siguiendo el art. 32 de la LAECSP, otro aspecto a tener en cuenta, es el hecho de que la remisión de expedientes podrá ser sustituida a todos los efectos legales por la puesta a disposición del expediente electrónico, teniendo el interesado derecho a obtener copia del mismo. Por lo tanto, se tendrán que establecer los medios necesarios para que un expediente electrónico esté accesible sólo para los que sean interesados, y para los que dentro de la Administración tengan derecho a acceder a él.

En base a esto, es muy útil estar en disposición, dentro del backoffice de la Entidad Local, de **un gestor de expedientes** que permita definir workflows de trabajo y roles, de manera que se automatice todo el trabajo interno de la Administración, facilitando incluso la puesta a disposición de los ciudadanos de la información relativa al estado de sus trámites, y por tanto a sus expedientes. Hay que recordar que en la LAECSP, se define como derecho de los ciudadanos, el hecho de poder acceder a la información sobre el estado de los trámites en los que figuran como interesados, pero no se determina cómo implementar este derecho. El gestor de expedientes es una buena herramienta para ello, pero no es la única forma de hacerlo. Hay que tener en cuenta, que poner en marcha esta herramienta requiere un proceso previo de reingeniería de procesos que incluye la racionalización y simplificación de procedimientos, que no es ni mucho menos un proceso banal.

A modo de resumen, los expedientes electrónicos que deban ser puestos a disposición deberán:

- Disponer de código para identificación.
- Llevar un índice electrónico, firmado electrónicamente.
- Disponer de una estructura y formato que se ajuste a lo que establezca el ENI.
- Estar integrados por documentos electrónicos que podrán formar parte de distintos expedientes y pueden incluir asimismo otros expedientes electrónicos.
- Ajustarse a formato o formatos de larga duración.

5.11 PUBLICACIONES ELECTRÓNICAS DE BOLETINES OFICIALES

Para impulsar la adaptación de las publicaciones oficiales al mundo electrónico, en el art. 11 de la LAECSP, se indica que las Administraciones Públicas competentes pueden publicar en **sus sedes electrónicas** los diarios o boletines oficiales, de manera que siempre que se disponga de las condiciones y garantías necesarias, **podrán tener la misma validez que en su versión en papel**.

Si nos centramos en el caso de las Entidades Locales, la publicación oficial por excelencia es el boletín oficial de la provincia, por lo tanto las Diputaciones Provinciales son las que en este caso toman un especial protagonismo. Si nos remitimos al art. 9 de la Ley 5/2002, de 4 de abril, reguladora de los Boletines Oficiales de las Provincias, son las Diputaciones las que impulsarán *"el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos en la prestación del servicios del Boletín Oficial de la Provincia"*, de manera que serán estas Diputaciones Provinciales los órganos competentes a la hora de elaborar y publicar estos boletines y diarios oficiales en la sede electrónica que tengan constituida, debiendo para ello, dotarse de las medidas de seguridad que garanticen la autenticidad e integridad de su contenido.

Para asegurar ese contenido, podemos remitirnos a las condiciones de publicación de la versión digital del BOE, determinadas en el Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial "Boletín Oficial del Estado". Donde, además de establecer el carácter oficial de esta publicación electrónica (art. 3), hay que destacar que, en cuanto a identificación se refiere:

- En su art. 12 se determina que esta edición deberá **incorporar firma electrónica avanzada** como garantía de la autenticidad, integridad e inalterabilidad de su contenido. En el caso del BOE, dicha firma se incorpora por separado en cada una de las disposiciones publicadas, esto permite asegurarse de la autenticidad de una disposición concreta sin necesidad de descargar el diario completo.

- En ese mismo artículo, se indica que los ciudadanos podrán verificar el cumplimiento de estas exigencias mencionadas en el punto anterior, mediante aplicaciones o herramientas informáticas que proporcione la sede electrónica de la Agencia Estatal Boletín Oficial del Estado, lo que viene a requerir **un servicio de verificación de esas firmas electrónicas**.

- En el art. 4, se determina **la inclusión de un código seguro de verificación** para que el ciudadano pueda contrastar la autenticidad de cualquier página del boletín.

- En el art. 21 se insta a la creación de unos registros de firmas digitales o, en su caso, manuscritas de las autoridades y funcionarios facultados para firmar la inserción de los originales destinados a publicación.

- En el art. 12 se establece la necesidad de **custodiar y conservar** la edición electrónica del diario oficial del Estado, así como velar por la accesibilidad de la edición electrónica y su permanente adaptación al progreso tecnológico. Con lo que indirectamente están haciendo referencia al uso de un formato y medidas adecuadas que permita un archivado de estos boletines con plenas garantías, bajo lo ya expuesto en el apartado dedicado al *"archivo electrónico".*

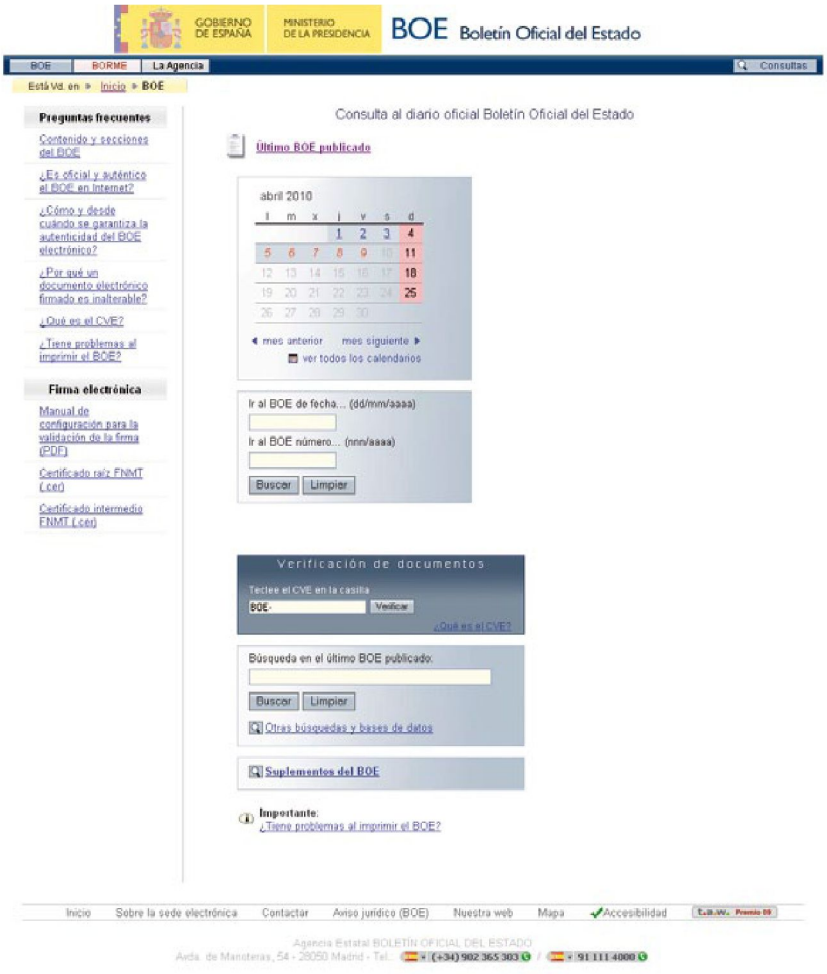


Fig.43

Portal web del Boletín Oficial del Estado

Estas consideraciones permiten sustraer los posibles aspectos a tener en cuenta cuando pretendamos publicar por ejemplo el boletín oficial de la provincia, caso en el que se encuentran todas las Diputaciones Provinciales:

- Que el boletín o diario oficial incorpore al menos la **firma electrónica avanzada**, como garantía de la autenticidad, integridad e inalterabilidad de su contenido. Además tenemos que considerar como buena práctica la incorporación de esta firma en cada una de las disposiciones por separado para permitir no tener que descargar el documento completo. Este hecho conlleva la necesidad de incorpora en la sede electrónica un **sistema que permita la verificación de estas firmas**.

- Incluir un **código seguro de verificación** que facilite el cotejo, y por tanto el acceso a través de la sede electrónica a **la aplicación que permita llevar a cabo ese cotejo**.

- Establecer las autoridades o funcionarios facultados para llevar a cabo esa firma.

- Se tiene que proceder al **archivado del boletín**, y por tanto a las consideraciones que esto conlleva.

5.12 PUBLICACIÓN ELECTRÓNICA DEL TABLÓN DE ANUNCIOS O EDICTOS

La publicación electrónica del tablón de anuncios o edictos va a permitir una mejor difusión de su contenido, en base a una mayor flexibilidad en el momento de acceder al mismo, lo que repercute directamente en la calidad del servicio ofrecido a ciudadanos y empresas. Además, gracias al art. 12 de la LAECSP, en el que se indica que *"la publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en el tablón de anuncios o edictos* ***podrá ser sustituida*** *o complementada por su publicación en la* ***sede electrónica*** *del organismo correspondiente"*, se consolida como un elemento más de la Administración Electrónica a la que queremos llegar.

Esta última consideración respecto a la posibilidad de la sustitución completa del tablón tradicional resulta controvertida, debido a que supondría suprimir el canal presencial. Como posible consecuencia se podría dejar sin acceso a ciudadanos que carecen de los medios o habilidades para utilizar los canales electrónicos, pudiendo llegar con ello a atentar **contra el principio de igualdad y no discriminación** en la elección del canal de relación con la Administración, reconocido en la propia LAECSP.

Esta situación podría evitarse simplemente poniendo a disposición de los ciudadanos un equipo informático en la oficina presencial que tenga habilitada la Entidad Local en cuestión. En él se podría visualizar la relación de anuncios publicados y acceder a cualquier anuncio completo, evitando los tradicionales tablones atiborrados de papeles cuya lectura resulta bastante farragosa.

Respecto a la implementación del tablón electrónico, podemos remitirnos a distintas normativas publicadas, como el Decreto de 21 de enero de 2010 del Vicealcalde por el que se aprueban las instrucciones para la implantación del Tablón de Edictos Electrónico del Ayuntamiento de Madrid, en el se establece, respecto a identificación electrónica, en el Anexo I apartado sexto:

- *"Se podrá consultar mediante el acceso a la página web del Ayuntamiento de Madrid, o cualquier otro que se determine"*. Pero en este caso, y de forma más clara nos podemos remitir al art. 12 de la LAECSP, en el que se determina que la publicación del tablón de anuncios o edictos en formato electrónico sea **accesible a través de la sede electrónica** del organismo correspondiente.

- Además se indica que el tablón *"dispondrá de los sistemas y mecanismos que garanticen la autenticidad, la integridad y la disponibilidad de su contenido en función de lo previsto en la Ley 30/92, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común"*. Por lo tanto el tablón **deberá contener copias electrónicas auténticas de los documentos a publicar o documentos electrónicos debidamente firmados**, con las implicaciones que esto conlleva y que ya han sido comentadas en apartados anteriores, de manera que los edictos y anuncios publicados cuenten con todas las garantías que acrediten su fehaciencia.

En la imagen que se adjunta a continuación, se muestra el funcionamiento del tablón de edictos del Departamento de Informática del Área de Gobierno de Hacienda del Ayuntamiento de Madrid.

Según este modelo, un emisor elabora un edicto y lo envía por correo electrónico en formato PDF a su unidad gestora correspondiente, adjuntando también una solicitud normalizada de publicación. Y una vez que el gestor de contenidos recibe la solicitud

Fig.44

Modelo de gestión del tablón de edictos del Departamento de Informática del Área de Gobierno de Hacienda del Ayuntamiento de Madrid

en un buzón de correo, da de alta y publica el anuncio, generando y remitiendo al solicitante la diligencia de exposición, una vez finalizado el periodo de vigencia.

A modo resumen, una Entidad Local que pretenda poner en marcha este tablón de anuncios o edictos electrónicos en materia de identificación debe contar:

- Con los sistemas de identificación y autenticación que permitan que los documentos publicados cuenten con todas las garantías, en función de la naturaleza de cada documento.

- Con un servicio accesible desde la sede electrónica, que permita el cotejo de los documentos electrónicos, y la validez de las firmas electrónicas que contengan.

CONCLUSIONES

La LAECSP ha supuesto un punto de inflexión para el impulso de la Administración Electrónica a todos los niveles, ya que en ella se reconoce por primera vez el derecho de los ciudadanos a relacionarse con la Administración por medios electrónicos. El ejercicio de este derecho lleva implícito la necesidad de desarrollar mecanismos que ofrezcan el mismo nivel de seguridad y garantía que en el caso de uso de medios no electrónicos, **siempre bajo el principio de proporcionalidad**, ya que cualquier duda de los ciudadanos a este respecto minaría el éxito de la incorporación de éstos a la Administración Electrónica. En este sentido, el desarrollo de las herramientas que den soporte a la identificación y autenticación electrónica está siendo uno de los obstáculos técnicos más significativos a los que se están teniendo que enfrentar todas las Administraciones Públicas, y que debe ser **abordado y solucionado con la mayor diligencia**, ya que en enero de 2010 ha entrado en plena aplicación la LAECSP.

Pero no es un reto únicamente técnico, sino que presenta aspectos organizativos y requiere una gran capacidad de comprensión e interpretación de las leyes que lo soporta, entre las que hay que destacar la **LFE**, en las que se asientan las bases de la identificación y autenticación electrónica, y la propia **LAECSP**, en la que aparecen nuevos conceptos y figuras que requieren de identificación y autenticación. Junto a esto, y también presentados en la LAECSP, se encuentran el ENS y el ENI, recientemente publicados, que añaden una capa más a esta torre normativa, determinando los criterios comunes de seguridad y de gestión de la información que permiten compartir soluciones y datos, y que por tanto determinan las pautas a seguir a la hora de identificarnos tanto dentro como fuera de nuestra propia Entidad.

Pero para superar este reto no podemos quedarnos aquí, su complejidad no se limita a aplicar una ley en sí misma, o a adquirir una determinada tecnología, sino que además requiere un profundo conocimiento de la Administración Pública. Este conocimiento forma parte del know-how de todos y cada uno de los miembros de la propia administración (empleados públicos, auxiliares, técnicos, políticos,...), y por tanto, es necesario el trabajo conjunto de áreas y personal de muy diversos perfiles, donde aspectos como el compromiso, la coordinación, la comunicación y el liderazgo son críticos, y pueden ser la diferencia entre el éxito y el fracaso. Además, es necesario que este conocimiento se aplique inicialmente a la realización de un **profundo análisis de**

la Administración que abarque tanto aspectos organizativos, como funcionales u operativos, por lo que es indispensable contar con la experiencia y colaboración de los empleados públicos, que conocen de primera mano esta realidad a todos los niveles.

Si nos centramos en las necesidades de identificación y autenticación, se tiene que poner a disposición de los distintos agentes que intervienen, las herramientas para que esto sea posible. Para ello hay que contemplar toda la casuística que gira en torno a las relaciones establecidas entre estos agentes (ciudadanos, empresas, empleados públicos y Administraciones Públicas), y que básicamente está agrupada alrededor de cuatro ejes: la relación entre ciudadanos y empresas con la Administración, la relación entre Administración con ciudadanos y empresas, la relación entre miembros de la propia Administración y la relación entre distintas Administraciones.

Como elementos técnicos que van hacer posible esta identificación y autenticación, hay que destacar desde el punto de vista del ciudadano, el uso del **DNIe**, además de los dispositivos y otras soluciones que se pongan a su disposición desde las Administraciones Públicas. En este caso, uno de los sistemas más relevantes para su identificación es el **certificado de sede electrónica**, ya que da soporte al más importante punto de acceso a los servicios de cada administración, su sede electrónica. Además, y como base para que la actuación administrativa automatizada sea posible, es necesario contar con el **certificado de sello electrónico y el código seguro de verificación**, que junto con el de sede, permiten a los ciudadanos y empresas no tener dudas respecto al organismo de la administración con el que se están relacionando.

Por último, otro papel destacado, debido tanto a su relevancia como a la complejidad técnica y organizativa que comporta, es el **certificado de empleado público**, para la identificación de los trabajadores de las administraciones en el desarrollo de su competencia.

Como hemos visto durante este documento, no hay una única solución para implementar cada uno de los casos que pueden presentarse en el día a día de una Entidad Pública, sino que del estudio de su idiosincrasia debe surgir la relación de herramientas y sistemas a aplicar, teniendo como referencia el abanico mostrado a lo largo de este documento y los comentarios hechos al respecto.

SÍMBOLOS

	Texto plano
	Texto cifrado
	Hash o resumen del texto plano
	Clave
	Clave pública
	Clave privada
	Usuario
	Certificado
	Firma Digital
	Sello de Tiempo
	Autoridad de Certificación (CA)
	Autoridad de Registro (RA)

BIBLIOGRAFÍA

Guía de Adaptación de las Entidades Locales a la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos

Autor: *Red de Municipios Digitales*

Publicado en: *www.jcyl.es/rmd*

Fecha de Publicación: *3 de septiembre de 2008*

Esquema de identificación y firma electrónica de las Administraciones Públicas

Autor: *Grupo de Identificación y Autenticación. Consejo Superior de Administración Electrónica. Ministerio de la Presidencia*

Publicado en: *www.ctt.map.es*

Fecha de Publicación: *versión del 20 de noviembre de 2009*

Guía para la aplicación de la Ley 11 en materia de gestión de documentos electrónicos, expediente electrónico y archivo electrónico

Autor: *Carlota Bustelo Ruesta y Elisa García-Morales (Inforárea S.L.). Ministerio de Presidencia*

Publicado en: *www.ctt.map.es*

Fecha de Publicación: *versión del 16 de julio de 2009*

La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos

Autor: *Eduardo Gamero Casado, Julián Valero Torrijos y otros*

Editorial: *Aranzadi SA*

Fecha de Publicación: *2008*

DNI electrónico. Guía de Referencia Básica

Autor: *Grupo de Trabajo de Comunicación y Divulgación. Comisión Técnica de Apoyo a la implantación del DNI electrónico. Ministerio del Interior*

Publicado en: *www.dnielectronico.es*

NORMATIVA

[1] *Ley 59/2003, de 19 de diciembre, de Firma Electrónica*

[2] *Real Decreto 1553/2005, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica*

[3] *Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos*

[4] *Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información*

[5] *Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrollo parcialmente la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos*

[6] *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*

[7] *Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica*

[8] *Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*

[9] *Real Decreto 209/2003 de 21 de Febrero por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos*

AVISO LEGAL

Junta de Castilla y León

red de municipios digitales de Castilla y León