Un paso electrónico: Infraestructuras y servicios comunes

Montaña Merchán Arribas

2013

Cuaderno 3: Identidad digital y firma electrónica

CONTENIDO

Cada vez más los ciudadanos utilizan medios telemáticos en sus relaciones tanto con las Administraciones, como con los bancos, comercio. En esta relación es imprescindible que el ciudadano o la empresa tengan confianza en que sus relaciones electrónicas con la Administración se efectúan con los mismos efectos que los trámites presenciales.

En el año 2012 ha aumentado en 5,6 puntos la población ha interactuado con las Administraciones Públicas a través de Internet. La mayoría, un 59,4% se relaciona para obtener información de sites web de la Administración, el 41,0% para descargar formularios oficiales y el 32,2% ha enviado formularios cumplimentados.

Sin embargo el 35,7%, de los 12,4 millones de usuarios de Internet que en los últimos 12 meses tuvieron necesidad de presentar formularios ante las administraciones públicas, no utilizaron Internet para tal propósito. Las principales razones aducidas por este colectivo fueron: no tiene firma o certificado electrónico (25,1%), porque lo tramitó por Internet otra persona en su nombre - un gestor, un asesor fiscal, un familiar o un conocido- (24,3%) y por falta de habilidades o conocimientos (21,1%).

Un colectivo de los ciudadanos, que tienen DNIe, desconocen que les proporciona un sistema de identificación y firma. La complejidad que presenta la utilización del DNIe es una barrera para su uso, por ello se han realizado varias acciones para paliarlo como el desarrollo de un asistente de instalación o un acuerdo con Microsoft para incluir los drivers en su sistema operativo.

1 NECESIDAD DE UNA IDENTIDAD DIGITAL.

Cada vez más los ciudadanos utilizan medios telemáticos en sus relaciones tanto con las Administraciones, como con los bancos, comercio. En esta relación es imprescindible que el ciudadano o la empresa tengan confianza en sus relaciones electrónicas con la Administración o las empresas privadas.

Esta confianza se basa en saber que los servicios electrónicos producen los mismos efectos que los servicios presenciales, que están disponibles y que la administración identifica al ciudadano.

Para este último punto es necesario disponer de instrumentos capaces de acreditar la identidad de los involucrados en las comunicaciones electrónicas, de asegurar la procedencia y la integridad de los mensajes intercambiados.

La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 diciembre de 1999, establece un marco comunitario para la firma electrónica, en el contexto de esta Directiva, el Estado español aprueba la Ley de Firma Electrónica, Ley 59/2003 de 19 de diciembre, y el RD del Documento Nacional de Identidad electrónico. La primera proporciona un marco legal para la firma electrónica y el segundo un instrumento para la identificación y firma a todos los ciudadanos.

El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, se aprobó 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 intentaba establecer rápidamente un marco jurídico para aportar confianza en la realización de transacciones electrónicas en Internet. Este Real Decreto Ley incorporó al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, **incluso antes** de su promulgación y publicación en el *Diario Oficial de las Comunidades Europeas.* No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000.

La Ley 59/2003 es el resultado de transponer la Directiva 1999/93/CE y de incorporar las modificaciones basadas en la experiencia acumulada desde 1999. En esta Ley se fija el marco normativo básico del DNI electrónico poniendo de manifiesto sus dos notas más características -acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

Adicionalmente, se añade un régimen especial para la expedición de certificados electrónicos a entidades **sin personalidad jurídica**, referidas en el artículo 33 de la Ley General Tributaria, a los efectos de su utilización en el ámbito tributario y se incluye la posibilidad de efectuar relaciones de representación que pueden subyacer en el empleo de la firma electrónica.

Siguiendo la pauta marcada por la *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

“El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio.”

Lo que llama la atención ya que debería ser el documento electrónico firmado la prueba documental independientemente del soporte, aunque es necesario alguno. Pues si en el caso de firma sobre papel no es posible separar el uno del otro en el caso de documento electrónico este puede presentarse en varios soportes.

2 CONCEPTO DE IDENTIDAD DIGITAL

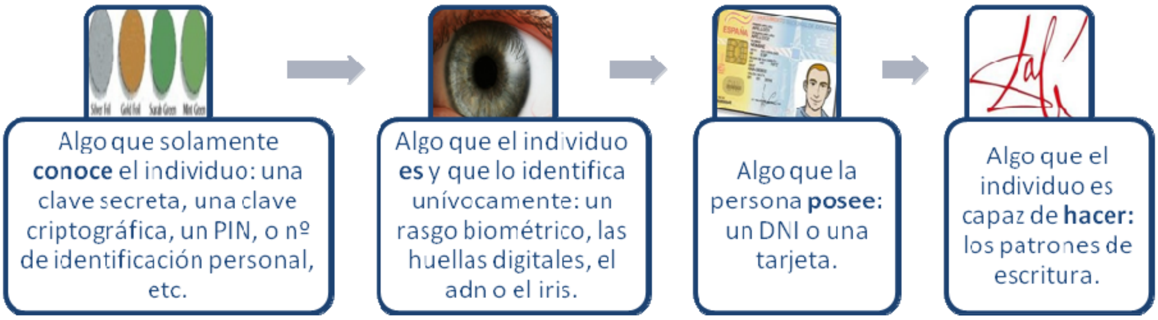
Antes de entrar en la materia de la identidad digital y la firma electrónica conviene diferenciar dos conceptos: la identificación y la autenticación.

- La identificación es la acción de darse a conocer ante el sistema
- La autenticación es la verificación que se realiza sobre esa identificación

En otras palabras la identificación es decir soy “fulano de tal” pero la autenticación es comprobar que efectivamente soy quien digo ser.

¿Cómo autenticamos a una persona? existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Mediante algo que solamente el individuo **conoce,** como una clave secreta de acceso, una clave criptográfica, un nº de identificación personal (PIN), etc.
2. Mediante algo que el individuo **es** y que lo identifica unívocamente: por ejemplo un rasgo biométrico como las huellas digitales, el adn o el iris.
3. Mediante algo que la persona **posee:** por ejemplo un DNI o una tarjeta.
4. Mediante algo que el individuo es capaz de **hacer:** por ejemplo los patrones de escritura.



Para la autenticación 2 y 3 necesitamos tener a la persona delante y compararlo con un patrón que un tercero certifica (la Dirección General de la Policía o tráfico, un perito grafólogo o la firma manuscrita del DNI). Con la 1 y 4 podemos identificarla a distancia por la password, la voz, la escritura (sin plantear cuanto de fácil puede ser su falsificación).

El España la identificación se hace mediante el DNI o el NIE que es un sistema de identificación basado en una tarjeta que emite el Ministerio de Interior, previa comprobación de forma presencial de ciertos rasgos que se incluyen en el mismo: la foto facial, la huella dactilar del índice y la firma manuscrita. De forma que presentando el DNI alguien puede contrastar estos rasgos directamente con la persona. El soporte del DNI es único e incorpora elementos que complica su falsificación.

La identidad digital debe proporcionar un método de autenticación de una persona sin necesidad de tenerla delante, de manera unívoca. La identificación digital y la firma electrónica surgen como respuesta a la necesidad de conferir seguridad a las comunicaciones por internet.

Para facilitar esta identificación y firma por internet se crea el Documento Nacional de Identidad electrónico (DNIe), como una adaptación del tradicional documento de identidad para la identificación tanto presencial como a distancia. Para ello debe cumplir con las mismas características: ser único, certificado por un tercero y no falsificable.

El DNIe se puede utilizar para identificarse o firmar en todas aquellas transacciones o intercambios que se realizan por medios telemáticos. La identificación y la firma electrónica que contempla la Ley de firma electrónica (LFE) están basados en certificados digitales y en claves simétricas por lo cual se da un breve información conceptual sobre estas herramientas.

3 CRIPTOGRAFÍA

Según la definición del diccionario, Criptografía es "El arte de escribir de un modo enigmático o con clave secreta, de modo que sea imprescindible ésta para descifrar lo escrito".

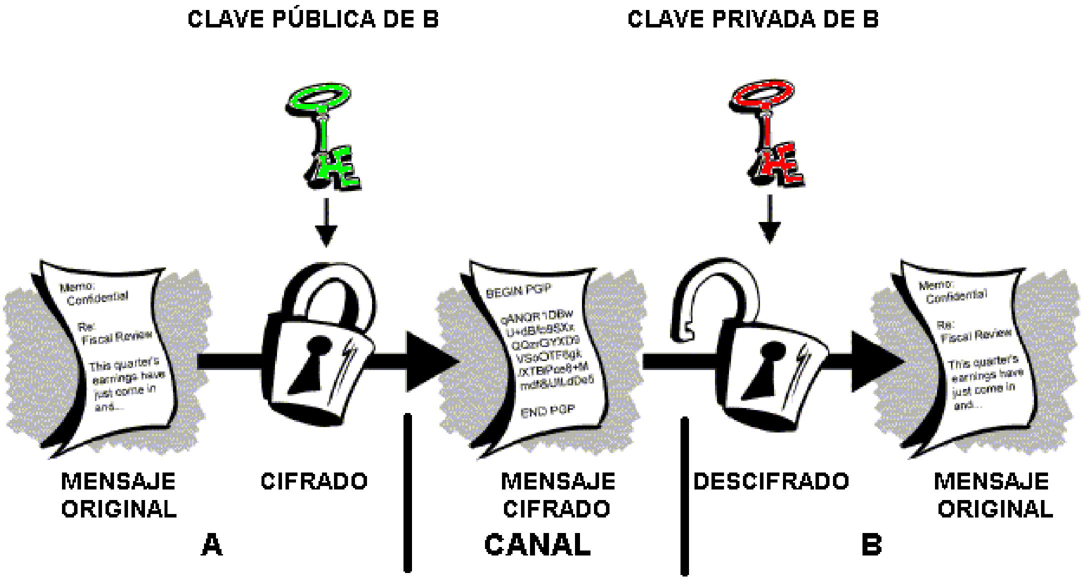
El objetivo principal del sistema criptográfico es ocultar la información a todo aquél que no conociera la clave para interpretar el criptograma. Esta función, se conoce como **privacidad**, pero no el único objetivo de la criptografía. Además, un sistema criptográfico, debe garantizar la **integridad** del mensaje, es decir, poder detectar si el mensaje ha sido alterado en el camino. En operaciones de comercio electrónico interesa que el sistema pueda saber que la persona que realiza la operación es quien dice ser, y no ha sido suplantada por otra. Esto es lo que se denomina **autenticidad** de origen. Evitar la suplantación es un punto a tener en cuenta cuando la compra o el asunto son importantes, y para evitar estafas, el que recibe el documento debe estar seguro de que quien lo envía no puede negar su autoría. Esto se conoce como “No repudio”. Estas cuatro premisas son fundamentales para poder llevar a cabo transacciones electrónicas importantes.

La criptografía llamada **asimétrica o de clave pública** permite garantizar los cuatro objetivos: Privacidad, integridad, autenticidad y no repudio. Cada persona tiene dos claves, una pública y otra privada. La pública es conocida por todos y la clave privada de cada persona, es conocida exclusivamente por él mismo. Esto hace que el sistema pueda garantizar la autoría de un mensaje sin lugar a dudas.

Si dos personas comparten una misma clave para intercambiar información confidencialmente, la criptografía se conoce como criptografía simétrica o de clave secreta, pero no se puede asegurar la autenticidad ni el no repudio.

La criptografía **asimétrica o de clave pública** es la que se utiliza en la firma electrónica y en la identificación basada en certificado digital.

La criptografía es una ciencia, basada en operaciones matemáticas que se aplican sobre los mensajes, independientemente de lo que contenga y que como resultado se obtiene una serie de ceros y unos.



El DNI-electrónico permite la identificación y la firma electrónica basándose en la criptografía asimétrica con dos claves: una privada y otra pública. Nunca debe darse la clave privada.

4 CERTIFICADO DIGITAL

El certificado digital o electrónico es *un documento expedido y firmado electrónicamente por un prestador de servicios de certificación que relacionan las herramientas de identidad o firma electrónica de un usuario, con su identidad, dándole a conocer como firmante en el ámbito telemático* (LFE).

Un certificado no es otra cosa más que un conjunto de datos vinculados a una identidad, la del titular o firmante, y esta relación está garantizada por un prestador de servicios de certificación. El certificado está firmado por este prestador.

Si se tiene instalado un certificado puede verse en el navegador.

Existen certificado reconocidos y no reconocidos. La diferencia es que los certificados electrónicos reconocidos se han expedido cumpliendo unos requisitos y se ha comprobado la identidad del firmante. Las condiciones se especifican en el artículo 11 de la Ley.

El Certificado Digital o Certificado de Clave Pública debe responder a formatos estándares reconocidos internacionalmente y contener, como mínimo, los siguientes datos:

a) Número de serie del certificado

b) Nombre de su titular
c) Tipo y número de documento del titular
d) Clave Pública del titular, identificando el algoritmo utilizado
a) La firma electrónica avanzada de la autoridad de certificación que emitió el certificado
b) Período de vigencia del certificado
c) La dirección de Internet de las condiciones de emisión y utilización del certificado
d) La dirección de Internet de la lista de certificados revocados que mantiene la Autoridad de Certificación (AC)
e) La dirección de Internet del manual de Procedimientos, Políticas de Certificación y Términos y Condiciones para la obtención de Certificados
f) Nombre de la Autoridad de Certificación (AC) que emitió el certificado

La Autoridad de Certificación, puede incluir información no verificada, debiendo indicar claramente tal circunstancia en las correspondientes condiciones de emisión y utilización del certificado.

El Certificado de Clave Pública es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio indicada en el certificado y finaliza en su fecha de vencimiento, o con su revocación si fuere revocado.

Los certificados reconocidos constituyen una pieza fundamental de la llamada firma electrónica reconocida, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y **generada mediante un dispositivo seguro de creación de firma**.

La firma electrónica que se realiza con un certificado reconocido se llama, firma reconocida y la Ley le otorga la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

La firma reconocida equivale a la manuscrita.

El certificado lo emite el prestador y puede enviarse (sin la clave privada) a un tercero. Nunca debe compartirse la clave privada.

4.1 Tipos de certificados

La Ley de firma define dos tipos de certificados

<u>Certificados de persona física</u>, es el que acredita la identidad de una persona.

<u>Certificados de persona jurídica</u> que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones. Podrán solicitarlos sus administradores, representantes legales y voluntarios con poder bastante a estos efectos. La Ley obliga a los solicitantes a responsabilizarse de la

custodia de los datos de creación de firma electrónica asociados a dichos certificados, sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad.

Los certificados de persona jurídica no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Los certificados de representante acreditan la pertenencia a empresa y también los poderes de representación que el titular tiene sobre la misma.

Certificados de entidades sin personalidad jurídica que identifica una asociación o comunidad de vecinos, etc

En el RD 1671/2009 se define además:

Certificado de empleado público que además de la identidad del titular acredita su vinculación con el organismo para la que trabaja y que pueden ser utilizado en el desempeño de las funciones propias del puesto que ocupen o para relacionarse con las Administraciones públicas cuando éstas lo admitan.

Certificado de sello de órgano que identifica un organismo público. Se utilizan para identificar y firmar actos administrativos por medio de sistemas informáticos sin intervención directa de la persona física competente.

Certificado de sede que sólo identifica la sede.

Aunque no está contemplado en la normativa, referenciamos el certificado de servidor web es aquel que permite identificar un servidor Web o una URL Este certificado le permitirá establecer comunicaciones con sus clientes utilizando la tecnología SSL, el estándar para comunicaciones seguras en la Web. Su servidor se identificará a los clientes con el nombre del dominio donde se encuentra su servicio Web.

4.2 El prestador de servicios de certificación.

Es aquella persona física o jurídica que, cumpliendo los requisitos que determina la legislación establecida sobre firma electrónica, está capacitado para emitir certificados electrónicos.

> En la legislación española a los prestadores de servicios de certificación se les denomina "terceras partes de confianza" o "prestador de servicios de certificación" (PSC). Esta denominación se origina por las propias funciones que realizan, y que está dirigida a que los usuarios de esta infraestructura tengan la seguridad de que el sujeto con el que se contacta es quién dice ser sin posibilidad de error.

Es importante seleccionar como tercera parte de confianza una que realmente nos ofrezca la suficiente garantía. Es importante seleccionar como tercera parte de confianza una que realmente nos ofrezca la suficiente garantía.

La Ley 589/2003, elimina el registro de prestadores de servicios de certificación, que publicaba el Ministerio de Justicia, y establece tan sólo un servicio de difusión de información sobre los prestadores que operan en el mercado, así como las características de los productos certificaciones y servicios con que cuentan para el desarrollo de su actividad. La lista de prestadores de certificación que cumplen con la Ley de firma electrónica, Ley 59/2003 de 19 de diciembre, se publica en el Ministerio de Industria, Turismo y Comercio.

https://sedeaplicaciones2.minetur.gob.es/prestadores/

Las funciones de la autoridad de certificación son emitir Certificados de Clave Pública de acuerdo a lo establecido en las condiciones de emisión y utilización de sus certificados, para lo cual debe:

a) recibir solicitudes de emisión de Certificado de Clave Pública;

b) numerar correlativamente los certificados emitidos;

c) mantener copia de todos los certificados emitidos, consignando su fecha de emisión, y de las correspondientes solicitudes de emisión.

La Autoridad de Certificación Abstenerse no puede acceder bajo ninguna circunstancia, a la clave privada de los titulares de los certificados que emita. Si el secreto de la clave privada se ve comprometido el certificado debe revocarse. L autoridad de certificación tiene la obligación de revocar los Certificados de Clave Pública por él emitidos en los siguientes casos:

a) a solicitud del titular del certificado.

b) solicitud justificada de un tercero.

c) si determinara que un certificado fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

d) si determinara que el criptosistema asimétrico de las claves públicas contenidas en los certificados emitidos ha dejado de ser seguro o si la función de digesto seguro utilizada para crear la firma digital del certificado dejara de ser segura.

La revocación debe indicar el momento desde el cual se aplica, precisando minutos y segundos, como mínimo, y no puede ser retroactiva o a futuro. El certificado revocado debe ser incluido inmediatamente en la lista de certificados revocados y la lista debe estar firmada por la Autoridad de Certificación.

La lista de certificados revocados debe publicarse en forma permanente e ininterrumpida en Internet.

Para que la firma electrónica sea válida el certificado debe estar vigente y no haber sido revocado.

De acuerdo con lo previsto en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, la autoridad de certificación debe publicar la **Declaración de Prácticas de Certificación (CPS)**. La CPS constituye el compendio general de normas aplicables a toda actividad certificadora de la Autoridad de Certificación. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Firmante/Suscriptor o Tercero que confía y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

La Autoridad de Certificación debe publicar, igualmente, la **Política de Certificación (CP)** que es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y utilización comunes.

En definitiva una Política define “**qué”** requerimientos de seguridad son necesarios para la emisión de los certificados. La Declaración de Practicas de Certificación nos dice “**cómo**” se cumplen los requerimientos de seguridad impuestos por la Política.

5 DNI ELECTRÓNICO

El Documento Nacional de Identidad es un documento con una antigüedad de más de 50 años, y está presente en la mayoría de las relaciones comerciales y administrativas, y su número figura como dato en el 97% de las bases de datos de entidades y organismos públicos y privados.

El Documento Nacional de Identidad es el único documento de uso generalizado en todos los ámbitos a nivel nacional y referente obligado para la expedición de otros documentos (pasaporte, permiso de conducir, seguridad social, NIF, etc.).

De esta forma se puede afirmar que el Documento Nacional de Identidad goza de una plena aceptación en la sociedad española.

A la hora de modernizar el DNI se plantea crear una DNI electrónico mejorando el servicio de expedición y aprovechando las ventajas de la tecnología para incorporar la firma electrónica.

El DNI electrónico acredita la identidad de datos personales de su titular y la nacionalidad española al igual que el DNI tradicional, pero añade las nuevas funciones de firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de firma electrónica. Esta característica se establece el artículo 2 del RD 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, "*Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo*".

La identificación mediante el DNI electrónico tendrá los mismos efectos que la identificación con el DNI tradicional sino también ante transacciones telemáticas. La firma electrónica de todo tipo de documentos electrónicos mediante el DNI electrónico, usando un dispositivo seguro de creación de firma tendrá efectos equivalentes a los de una firma manuscrita.

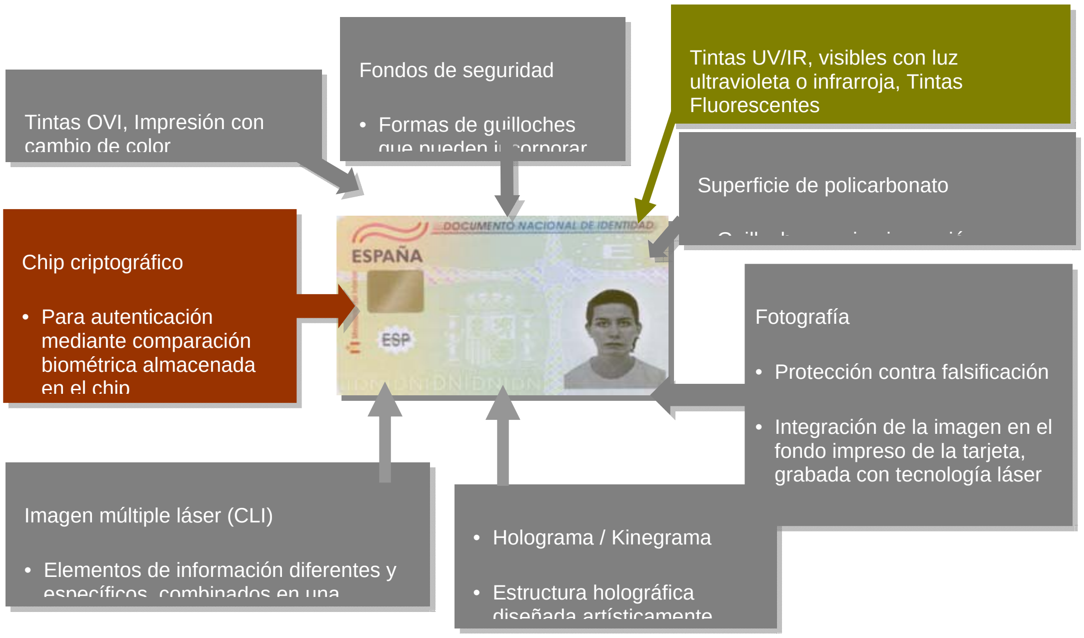
Hay más de 400 servicios de las Administraciones Públicas que admiten DNI electrónico para identificarse o firmar.

5.1 ¿Cómo es y qué contiene el DNI electrónico?

La tarjeta soporte del DNIe contiene los datos de filiación del ciudadano, los datos biométricos (modelo dactilar, foto y firma manuscrita) y los dos pares de claves RSA con sus respectivos certificados (autenticación y firma). Esta tarjeta está compuesta de 2 partes:

1. Tarjeta física del DNI electrónico.

Está fabricada en policarbonato y en el cuerpo de la tarjeta lleva grabada con láser de los datos de filiación, fotografía y firma manuscrita. Se le han añadido medidas de seguridad ante la manipulación y falsificación del documento, muchas de ellas fácilmente identificables sin ningún procedimiento especial.



2. Un chip

El DNIe incorpora un pequeño circuito integrado (chip), que contiene los mismos datos que aparecen impresos en la tarjeta (datos personales, fotografía, firma digitalizada, huella dactilar digitalizada) junto con los certificados de Autenticación y de Firma Electrónica.

Para leerlo requiere un lector de tarjetas inteligentes que cumpla el estándar ISO-7816.

El DNI electrónico contiene dos certificados X509v3 de ciudadano (autenticación y firma) y claves privadas asociadas, que se generarán e insertarán durante el proceso de expedición del DNI electrónico:

- El Certificado de autenticación sirve para certificar su identidad frente a terceros, demostrando la posesión y el acceso a la clave privada asociada a dicho certificado y que acredita su identidad.

- El Certificado de firma electrónica reconocida, permite realizar y firmar acciones y asumir compromisos de forma electrónica, pudiéndose comprobar la integridad de los documentos firmados haciendo uso de los instrumentos de firma incluidos en él. La firma este certificado es equiparable legalmente con la Firma Manuscrita (Ley 59/2003 y Directiva 1999/93/CE).

El PIN es la contraseña personal que (una vez comprobada por el microprocesador incluido en el chip) permite protege las claves privadas y, por tanto, es confidencial, personal e intransferible.

En el momento de la expedición, se genera un PIN aleatorio que se entrega al ciudadano en forma de "sobre ciego". El titular del DNI electrónico puede cambiar esta contraseña o PIN por cualquier otro de su elección en los Puntos de Actualización del DNI electrónico (PAD) existentes en las Oficinas de Expedición y en internet.

Si se olvida o se bloquea el PIN puede modificarse leyendo la huella dactilar con un lector de impresión dactilar, lo que permite acceder a los datos del chip.

5.2 Instalación

Para usar el DNIe es necesario instalar un lector de chip y los drivers del DNI.

Para simplificar el proceso se ha desarrollado un asistente del DNIe que ayuda en la instalación del lector de DNI y de sus drivers. El Asistente de Instalación del DNIe es un programa que te permitirá lo siguiente:

- Comprobar el estado de una instalación anterior del DNI Electrónico en su ordenador.

- Instalar todos los elementos necesarios para poder utilizar el DNI Electrónico.

- Utilizar el DNIe en los navegadores más habituales (Internet Explorer, Firefox y Chrome).

- Validar los certificados del DNI Electrónico.
- Desinstalar el DNI Electrónico en su equipo Windows o Linux (Ubuntu).

La descarga del asistente se hace desde http://zonatic.usatudni.es/

6 FIRMA ELECTRÓNICA.

La Directiva 1999/93/CE, de 13 de diciembre, establece un marco comunitario para la Firma Electrónica es imperativa ya desde su propio preámbulo, cuando contempla que "*La firma electrónica se utilizará en el sector público en el marco de las administraciones nacionales y comunitaria y en la comunicación entre dichas administraciones y entre éstas y los ciudadanos y agentes económicos, por ejemplo en la contratación pública, la fiscalidad, la seguridad social, la atención sanitaria y el sistema judicial*".

La legislación comunitaria y la estatal llevan ya varios años impulsando la utilización de la Firma Electrónica como medio de relación entre los ciudadanos y las diferentes administraciones y entre éstas.

La Ley 59/2003, de 19 de diciembre, de firma electrónica define la firma electrónica de la siguiente manera:

(Art. 3.1) La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. Permite autentificando las comunicaciones generadas por el firmante.

Los "datos de creación de firma" son los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica. El "firmante" es la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa.

Las principales funciones de la firma son:

- Identificación del firmante: la firma identifica al firmante de forma única igual que su firma manuscrita.
- Integridad del contenido firmado: es posible verificar que los documentos firmados no hayan sido alterados por terceras partes.

- No repudio del firmante: un documento firmado electrónicamente no puede repudiarse por parte de su firmante.

La firma permite que tanto identificar al emisor de un contenido con la certeza de que es él el que está interactuando, evita que terceras personas intercepten esos contenidos y que puedan ser alterados, así como que alguna de las partes "repudie" la información que recibió de la otra y que inicialmente fue aceptada.

6.1 Tipos de firma legales.

La Ley de firma electrónica distingue entre “firma simple”, “firma electrónica avanzada” y “firma electrónica reconocida”:

Art. 3.1) define firma simple 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*.

(Art. 3.2) La firma electrónica avanzada *es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control*.

(Art. 3.3) Se considera firma electrónica reconocida *la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*.

Un "dispositivo de creación de firma": un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma.

Nuestra legislación interna, de acuerdo con lo preceptuado en la Directiva (art. 5), concede validez y efectos amos tipos de Firmas Electrónicas, siendo aquellos plenos en el caso de la firma reconocida ya que se le otorga "*el mismo valor jurídico que la firma manuscrita*" en relación con los consignados (art. 3.4 Ley 59/2003) y se establece que "*los documentos que incorporen la firma reconocida serán plenamente admisibles como prueba en juicio*" (art. 3.8 Ley 59/2003).

Además, a la firma simple "no se le negarán, por el mero hecho de presentarse de esta manera (y no en papel) efectos jurídicos, ni será excluida como prueba de juicio" (art. 5.2 Directiva 1999/93 y 3.9 Ley 59/2003).

Es decir la firma puede no estar basada en certificado reconocido que no se niegue eficacia jurídica, ni la en un certificado expedido por un proveedor de servicios de certificación Acreditado y ser admitida como prueba en procedimientos judiciales.

En el portal de firma electrónica se publica un tutorial para aprender a firmar.

6.2 Funcionamiento de la firma electrónica

El modo de funcionamiento de la firma electrónica basado en clave pública es el siguiente:

- Cada parte tiene un par de claves, una se usa para cifrar y la otra para descifrar.
- Cada parte mantiene en secreto una de las claves (la clave privada) y pone a disposición del público la otra (la clave pública).
- Comienza el proceso de firma de un documento obteniendo un resumen del mismo a través de una función de Hash.

- El resultado obtenido es un conjunto de datos de tamaño fijo ya que estas funciones cuando se aplica originan siempre un resultado un tamaño fijo, independientemente del tamaño original.
- La propiedad más importante de ese resumen o Hash es que es unidireccional, del resultado no puede deducirse el contenido original y que dos documentos diferentes siempre producen resúmenes diferentes. Es

casi imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la función "hash".

- El emisor cifra el resumen del mensaje con la clave privada. El resumen cifrado con la clave privada es la firma electrónica y se añade al mensaje original.

El receptor, al recibir el mensaje, descifra la firma utilizando la clave pública del emisor obteniendo el resumen que el emisor calculó; calcula de nuevo su resumen mediante la función "hash", si ambos coinciden la firma es válida por lo que cumple los criterios ya vistos de autenticidad e integridad además del de no repudio ya que el emisor no puede negar haber enviado el mensaje que lleva su firma.

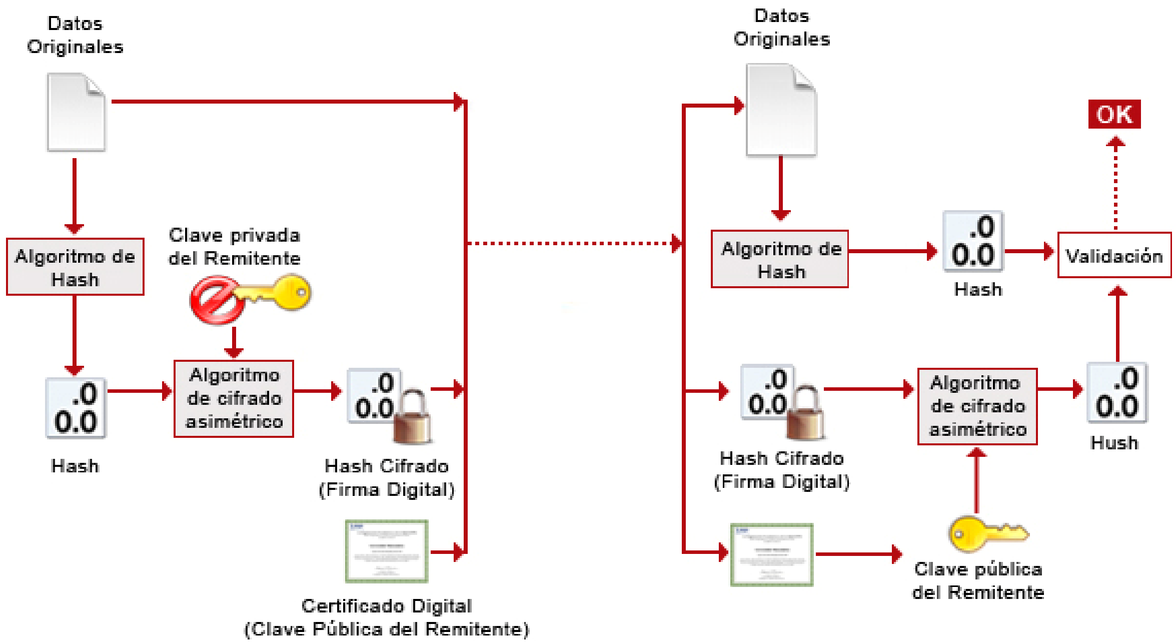


Imagen de Inteco

6.3 Formatos de firma electrónica

Se puede firmar documentos en diferentes formatos como doc, pdf, xml, etc, obteniendo un documento firmado electrónicamente que puede guardarse en distintos formatos de firma, que están definidos por estándares. Hay tres familia de formatos:

XAdES (XML Advanced Electronic Signatures), según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2. En este tipo de firmas el fichero con la firma es un XML. Los documentos a firmar pueden tener cualquier formato.

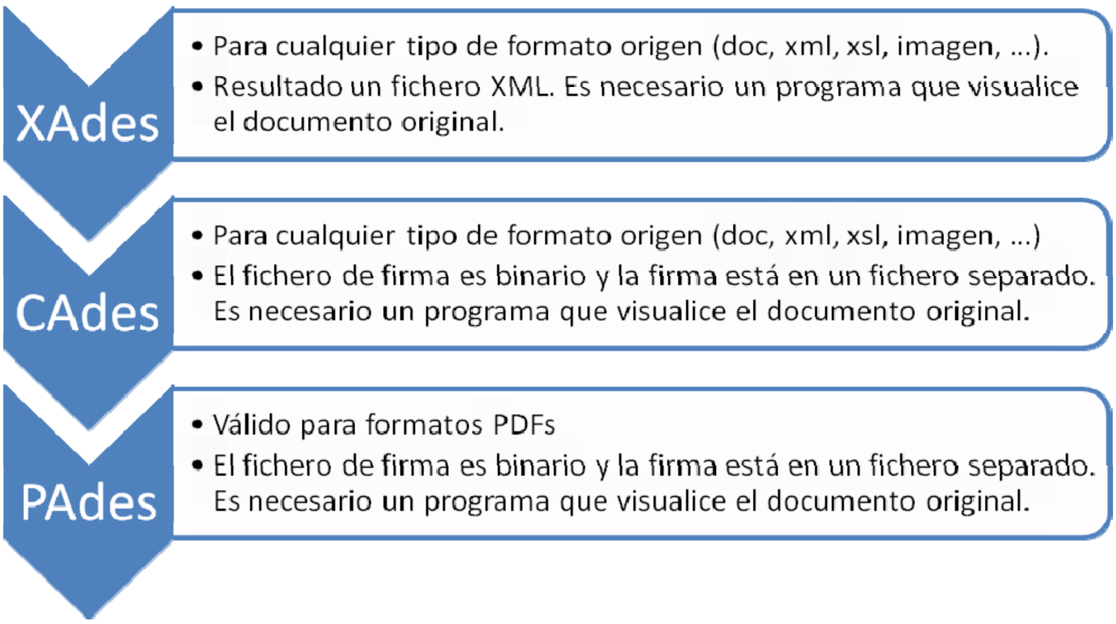
CAdES (CMS Advanced Electronic Signatures), según especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.4. El fichero de firma es binario y la firma está en un fichero separado. Se mantiene el documento original y la firma en un mismo fichero.

PAdES (PDF Advanced Electronic Signatures), según especificación técnica ETSI TS 102 778-3, versión 1.1.2. La firma está incluida en el estándar ISO PDF. Sólo se pueden firmar documentos PDF.

Con Adobe Acrobat también es posible firma un documento PDF, en formato propietario de Adobe e incluir una imagen.

Para los formatos CADES y PADES existen dos modalidades para guardar la firma: generar un único fichero resultante que contiene el documento original, y las firmas, encontrándose al mismo nivel XML lo firmado y la firma (attached) o dos ficheros, uno contienen la firma y el otro el documento (detached).

En resumen



Cada formato deriva en varios perfiles cuando se añade información, como sellos de tiempo (*timestamps*), referencias al estado de revocación de los certificados o a políticas de firma, etc…

Se define seis formas con distinto nivel de protección. Cada perfil incluye y amplía el anterior:

Cades	Xades	la forma básica sólo satisface los requisitos legales de la Directiva para la firma electrónica avanzada;
CAdES-T	XAdES-T	(fecha y hora), la adición de campo de fecha y hora de proteger contra el repudio;
CAdES-C	XAdES-C	(completa), la adición de referencias a los datos de verificación (certificados y listas de revocación) a los documentos firmados para permitir la verificación off-line y la verificación en el futuro (pero no el almacenamiento de los datos reales de verificación);
CAdES-X	XAdES-X	(ampliado), la adición de marcas de tiempo en las referencias introducidas por CAdES-C para proteger en el futuro el posible compromiso de los certificados de la cadena;
CAdES-XL	XAdES-XL	(ampliado a largo plazo), la adición de certificados reales y listas de revocación en el documento firmado para permitir la verificación en el futuro, incluso si su fuente original no está disponible;
CAdES-A	XAdES-A	(archivado), posibilidad de añadir periódicamente un sellado de tiempo (por ejemplo, cada año) en el documento archivado para evitar el compromiso causado por el debilitamiento de la firma durante un período de almacenamiento a largo plazo.

6.4 Firmas “longevas”

El proceso de verificación de una firma debe poder repetirse años después de su generación y con el paso del tiempo, los certificados caducan o incluso podemos no tener acceso a determinados datos necesarios para la comprobación.

Para solucionar este problema se incorporan a la firma electrónica información acerca de cuándo se produjo y elementos que permitan verificar esa firma sin ayuda externa, se deberán guardar y mantener todas las evidencias que posibilitarán su verificación posterior.

Formato de firma longeva EPES –XL: Añade los propios certificados y la información de revocación de los mismos para permitir la verificación en el futuro incluso si las fuentes originales no estuvieran ya disponibles

6.5 Política de firma

Con esta variedad de formatos, formas y versiones para asegurar la interoperabilidad, es decir que un organismo puede procesar los documentos firmados de otro, es necesario definir una serie de criterios y perfiles. Estos criterios se recogen en la **política de firma**.

El artículo 24.1 del RD 1671/2009 indica que la política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

Esta política representa el conjunto de criterios comunes de interoperabilidad asumidos por la Administración General del Estado (AGE) en relación con la generación y validación de firmas electrónicas basadas en certificados electrónicos y que afecta por tanto a las relaciones de la Administración con los ciudadanos y entre sus distintos órganos. El objetivo principal es facilitar el uso de firmas electrónicas seguras e interoperables entre los distintos departamentos y organismos de la AGE.

La política de firma electrónica se circunscribe a los certificados electrónicos previstos en la Ley 11/2007 expedidos para su empleo por la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta y a los sistemas de firma electrónica basados en certificados recogidos en el artículo 10.1 y 10.2 del RD 1671/2009.

El objetivo de este proceso es determinar la información que debiera incluir el firmante en el proceso de generación de la firma, y la información que debiera comprobar el verificador en el proceso de validación de la misma.

6.6 Validación

Igual que la firma manual la firma electrónica debe poder validarse. Para que una firma sea válida debe comprobarse primero la integridad de los datos firmados asegurando que éstos no hayan sufrido ninguna modificación y segundo que el certificado era válido en el momento de la firma.

Para realizar la validación de los certificados cada Autoridad de Certificación debe publicar la lista de los certificados revocados o caducados, bien mediante:

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

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

Las plataformas de validación de certificados se han desarrollado para facilitar a las aplicaciones la verificación de todos los certificados de las distintas Autoridades de Certificación, sin tener que conectar con cada una. Esto es precisamente el objeto de la plataforma @firma.

Verificación del DNI electrónico

En la Infraestructura de Clave Pública adoptada para el DNI electrónico, se ha optado por asignar las funciones de Autoridad de Validación a entidades diferentes de la Autoridad de Certificación, a fin de aislar la comprobación de la vigencia de un certificado electrónico de los datos de identidad de su titular.

La Autoridad de Certificación es el Ministerio del Interior – Dirección General de la Policía y de la Guardia Civil, mientras que la de validación son el Ministerio de Política Territorial y Administración Pública (para la administración) y la Fabrica Nacional de Moneda y Timbre (para ciudadanos, empresas, administración), de este modo el Ministerio de Interior no tiene en modo alguno acceso a los datos de las transacciones que se realizan con el DNIe y las Autoridades de Validación no tiene acceso a la identidad de los titulares de los certificados electrónico que maneja, reforzando –aún más si cabe- la transparencia del sistema.

7 PLATAFORMA DE VALIDACIÓN @FIRMA.

Cuando el ciudadano interacciona con la Administración, para realizar un trámite personal, es necesario conocer su identidad, que telemáticamente se realiza a través del DNI electrónico o un certificado electrónico. La Administración comprueba que el certificado o el DNIe con el que el ciudadano se está identificando o firmando la solicitud es válido y está vigente.

Para esta comprobación se utiliza la plataforma de validación @firma del MAP. La plataforma está operativa desde marzo de 2006. El objetivo de esta plataforma de validación es comprobar que el certificado utilizado por el ciudadano es un certificado válido y que no ha sido revocado y que por tanto sigue teniendo plena validez para identificar a su propietario.

Una plataforma de validación cumple unas finalidades esenciales:

Verifica	•la identidad electrónica de una persona con independencia del tipo de certificado que ésta utilice.
Valida	•los certificados electrónicos permitiendo el uso de los servicios.
Firma:	•La plataforma ofrece un Cliente de firma que permite a los ciudadanos firmar documentos electrónicos con destino a la Administración Electrónica y también ofrece la validación de firma de un elemento firmado, indicando si la firma es correcta y la validez, fechado de tiempo, etc
Sellado de Tiempo (TSA)	•Se incluye un servicio para certificar temporalmente todas las operaciones de validación y firma que se realizan a través de la plataforma (según el estándar RFC 316).
Gestión y administración	•La plataforma realiza la administración de los Prestadores de Servicios de Certificación adheridos y registra todas las operaciones realizadas para la auditoria y trazabilidad del sistema.

La plataforma ha sido galardona con el premio “best practice de la Unión Europea.

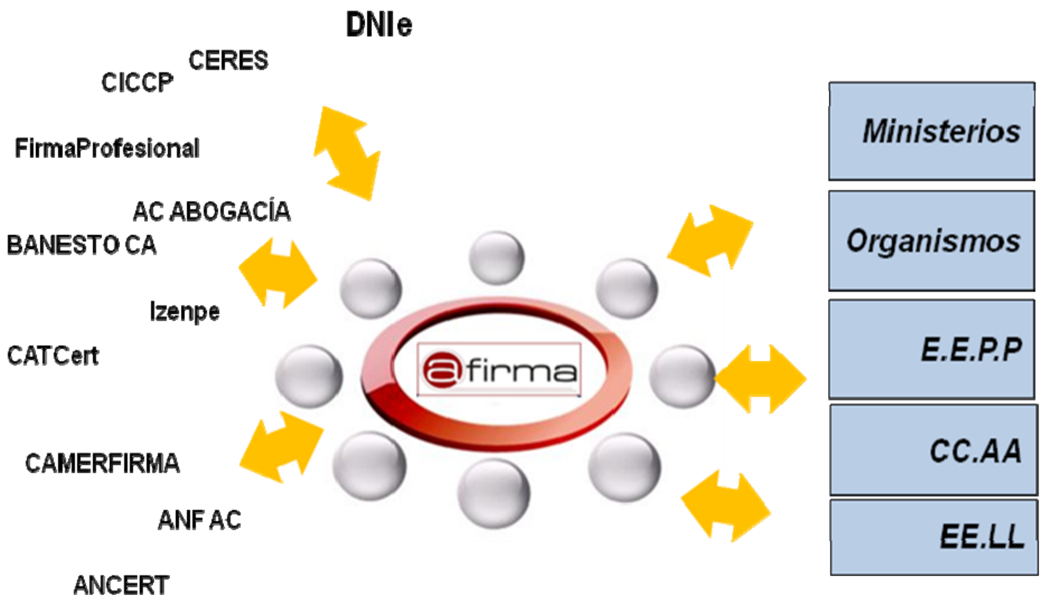
7.1 Beneficios de la plataforma

@firma, plataforma que permite validar tanto el DNIe como los más de 80 tipos de certificados reconocidos, emitidos por los prestadores privados reconocidos por el

Ministerio de Industria Turismo y Comercio u otros prestadores de certificados digitales.

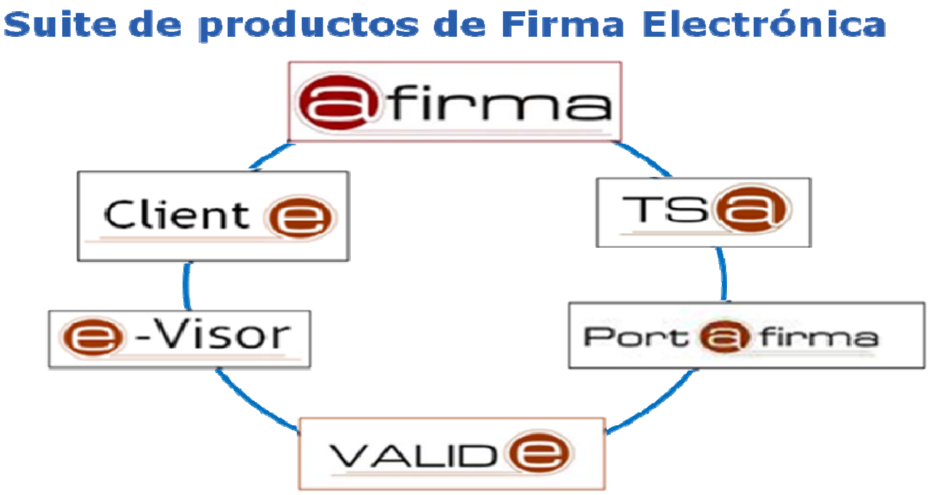
Los beneficios que la plataforma facilita a los organismos son:

- El reconocimiento de múltiples certificados con independencia del prestador de servicios de certificación y el soporte de varios protocolos de validación de certificados (OCSP, HTTP, LDAP).
- Garantiza la confidencialidad, autenticidad e integridad de todas las transacciones realizadas.
- Hace transparente para las aplicaciones el uso de diferentes formatos de firma electrónica como PKCS#7, CMS, XML signature, XAdES y CAdES
- Se perfila como el punto central para ser la plataforma de reconocimiento en el ámbito Europeo.



7.2 Servicios de identidad y firma

Las Administraciones Públicas cuenta con una suite de productos que dan solución a la Validación de certificados digitales, la firma electrónica el sellado de tiempo:



PLATAFORMA @FIRMA que es una aplicación para validar los cualquier certificado de cualquier prestador incluido en la lista del Ministerio de Industria, Comercio y Turismo y realizar la firma.

CLIENTE de firma que es una aplicación para instalar en el ordenador y permite firmar cualquier documento y comprobar la firma.

@TSA y efectuar sellados de tiempo (TSA), así como efectuar la comprobación electrónica de la fecha en la que se ha hecho una operación. La TSA lleva realizados 15 millones de sellados de tiempo.

VALIDE es un servicio web para el ciudadano y funcionarios que permite, no solo comprobar su certificado sino firmar un documento y validar un la firma en un documento firmado electrónicamente. Está públicamente disponible en la siguiente URL: https://valide.redsara.es

PORTAFIRMA para facilitar a las unidades administrativas el uso de la firma electrónica reconocida de documentos procedentes de diferentes sistemas de información independientes. Conlleva agilizar los procedimientos de la actividad administrativa.

7.3 Datos de la plataforma

La Plataforma de validación, @firma, es utilizada por 842 organismos (148 de la AGE, 70 de CCAA, 576 Entidades Locales y 49 de otras entidades). En 2011 lleva 50 millones de validaciones de certificados electrónicos, casi duplicando los 28 millones de 2010.

La TSA lleva realizados 15 millones de sellados de tiempo.

SE ha desarrollado una “Guía de uso del sello de tiempo y marca de tiempo. Uso de la TS@” que se puede descargar desde

http://administracionelectronica.gob.es/recursos/pae_000022132.pdf

VALIDE Es un servicio web para el ciudadano y funcionarios que permite:

- Comprobar si está vigente cualquier tipo de certificado;
- comprobar si es válido el certificado de una sede electrónica sin más que introducir la dirección de la sede;
- firmar un documento en los formatos que admite la Administración;
- validar y visualizar la firma en un documento firmado electrónicamente.

En el portal de firma electrónica puede descargarse la aplicación FirmaFácil, una aplicación de firma, que permite firma cualquier documento en el ordenador personal. Uso muy sencillo.

7.4 Firma en movilidad

La movilidad está adquiriendo una importancia creciente en el entorno de la empresa. El teléfono móvil es prácticamente una herramienta universal. El mercado español fomenta el modelo de Internet en movilidad. España se posiciona como el segundo país de Europa en venta de terminales inteligentes.

La penetración en el mercado de dispositivos de última generación (PDA’s teléfonos, etc) y de las tablets permiten a los usuarios acceder a diferentes aplicaciones tanto de ocio como corporativas desde cualquier sitio. Según la AIMC, uno de cada dos usuarios de telefonía móvil accede a los contenidos de diarios online desde su terminal. De las corporativas la más habitual es el correo electrónico.

Una de las perspectivas que se abre con estos dispositivos es el acceso del ciudadano a las aplicaciones de la administración electrónica a partir de estos dispositivos. En este caso, en muchos de los formularios que se utilizan es necesaria la identificación y la firma electrónica. Todos los altos cargos disponen de estos dispositivos y pueden acceder a aplicaciones corporativas. Entre ellas, podemos disponer un portafirmas que centralice las firmas de cualquier aplicación o empleado en nuestra carpeta.

En el caso de dispositivos móviles la seguridad tiene una gran importancia y los certificados digitales pueden aportar ventajas bien conocidas. Se plantean diversas soluciones para realizar la firma en estos dispositivos.

Los operadores principales de telefonía móvil han trabajado, junto con la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM), en la incorporación de certificados digitales dentro de sus tarjetas SIM, para permitir la identificación y la firma electrónica en el móvil. La ventaja de esta solución es su independencia de los diversos dispositivos y de la multiplicidad de sistemas operativos o navegadores. No obstante dicha tarjeta supone un incremento de coste respecto a la tarjeta común e implica pasar por el servidor de la operadora. Esta firma en dos fases exige para usarla, modificar las aplicaciones de administración electrónica que ya se tenga implementado.

Otra alternativa por la que se puede optar es realizar la firma completamente en el servidor, instalando un HSM, "**H**ardware **S**ecurity **M**odule" (Módulo de Seguridad Hardware). Los certificados de los usuarios se custodian en el HSM y se pueden activar por una clave más o menos compleja y segura. La ventaja es que es simple de utilizar para el ciudadano, aunque es necesario el registro del certificado en el organismo. Su seguridad está condicionada por la de la clave y el organismo tiene la responsabilidad del "no repudio". Es, sin embargo, una excelente solución para implementar la firma electrónica de los empleados dentro de una corporación.

Cuando se trata de dar la posibilidad a los empleados de utilizar la firmar en las aplicaciones corporativas, pueden implementarse distintas soluciones, además de las dos anteriores. Será muy útil disponer de una aplicación de portafirmas que centralice todos los documentos a firmar y que se adapte a los diversos dispositivos. La solución debe permitir conectarse al portafirma, revisar los documentos y firmarlos con su certificado digital. La firma puede hacerse en dos fases: la parte de la firma la gestiona la aplicación cliente en el móvil y las operaciones más pesadas se completan en el portafirmas.

Por supuesto, se puede realizar la firma completa en el dispositivo siendo necesario un cliente de firma específico. La ventaja es que no sería necesario modificar las aplicaciones y la seguridad está garantizada ya que la certificado lo custodia su propietario, el inconveniente es la falta de estandarización en los sistemas operativos y navegadores en los móviles, además de la variabilidad de las versiones de las aplicaciones y que es un entorno muy dinámico, **poco estable**. Esta es una solución factible para todos los colectivos y sin duda un línea de futuro.

En el mercado existen servicios de firma electrónica como viafirma o isigma. Moviestar o Vodaphone comercializan las tarjetas SIM con certificado. El Ministerio de Hacienda y Administración Pública está desarrollando un cliente de firma para Android y Apple iOS.

8 USO DE DNI ELECTRÓNICO EN EUROPA

El desarrollo del proyecto Stork supondrá para España la aceptación de los certificados digitales españoles, como los del DNI electrónico en servicios de Administración electrónica de otros países, lo cual facilitará la relación de nuestros ciudadanos y empresas con otras AAPP europeas.

El proyecto STORK (Secure idenTity acrOss boRders linKed) se desarrolla bajo la iniciativa "i2010 - A European Society for growth and employment", lanzada por la Comisión Europea en junio del 2005. Se enmarca en el programa de la Comisión Europea sobre Innovación y Competitividad (CIP) y es cofinanciado por ella. Está formado por un total de 29 Administraciones Públicas y empresas Europeas relevantes en materia de identificación electrónica, entre las que se encuentra el Ministerio de Política Territorial y Administración Pública.

El objetivo es facilitar que ciudadanos y empresas puedan utilizar sus identidades electrónicas en los servicios de eGovernment en cualquier estado miembro de la Unión Europea. Busca obtener el reconocimiento paneuropeo de las identidades electrónicas (eID) de manera transfronteriza.

Durante los tres años de duración se han elaborado unas especificaciones técnicas y comunes en toda Europa y se ha implementado unos sistemas para el reconocimiento de las diferentes eID y la autenticación electrónica. El objetivo último de STORK es armonizar y conectar los sistemas de identificación de los estados miembros del consorcio, sin sustituir los ya existentes. La solución técnica se testa a través de los pilotos implantados en servicios reales de administración electrónica.

El 25 de octubre de 2010 se pusieron en marcha 6 pilotos reales basados en 6 servicios de Administración electrónica. En dos de ello participa España: el de Comunicación de cambio de Domicilio; y el de Movilidad de Estudiantes, liderado por la Conferencia de Rectores de la Universidades Españolas (CRUE).

Los pilotos han demostrado que la interoperabilidad de identidades electrónicas es factible en servicios de administración electrónica. Favorecen la movilidad de los ciudadanos, y en especial los trabajadores, en toda la zona Euro.

La Universidad Jaume I ha participado en el piloto de movilidad de estudiantes. Actualmente se admiten las credenciales de Finlandia, Grecia, Lituania y Eslovaquia. (https://xmlrpc.uji.es/lsm/lsmanage.php?Tok=8f28a6abb7c41c1067810b2d4a&lang=ca)

El piloto de Comunicación de cambio de Domicilio permite a ciudadanos extranjeros, usando sus credenciales nacionales, notificar su cambio de domicilio a los organismos correspondientes.

El concepto del STORK es un paso importante para el desarrollo del mercado único europeo y la movilidad de los ciudadanos y permitirá que entidades privadas desarrollen nuevos modelos de negocio, basados en este método seguro de identificación transfronteriza de ciudadanos.

Por ello se ha integrado en la ventanilla EUGO.es con objeto de admitir en la tramitación, las identidades electrónicas de los prestadores de otros países.

Sitios de referencia

Lista de prestadores de certificación	https://sedeaplicaciones2.minetur.gob.es/prestadores/
DNI electrónico	http://www.dnielectronico.es/
Usa tu DNI	http://www.usatudni.es/dnie/
VALIDE	https://valide.redsara.es/valide/
Portal de firma electrónica	http://firmaelectronica.gob.es/
Firma fácil	Zona de descargas en http://firmaelectronica.gob.es/
Zona TIC	http://zonatic.usatudni.es/
Ley 59/2003	http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399
Ley 11/2007	https://www.boe.es/buscar/doc.php?id=BOE-A-2007-13411
RD 1671/2009	http://www.boe.es/boe/dias/2009/11/18/pdfs/BOE-A-2009-18358.pdf
Piloto de movilidad de estudiantes	https://xmlrpc.uji.es/lsm/lsmanage.php?Tok=8f28a6abb7c41c1067810b2d4a&lang=ca
Guía de uso del sello de tiempo y marca de tiempo. Uso de la TS@	http://administracionelectronica.gob.es/recursos/pae_000022132.pdf
Política de certificación del DNIe	http://www.dnielectronico.es/dpc
Declaración de certificación de camerfirma	http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_V_3_2_3.pdf
Declaración de certificación de CERES	http://www.cert.fnmt.es/dpc/dgpc.pdf
Política de certificación de CERES-APE	http://www.cert.fnmt.es/dpc/ape/dpc.pdf