INTECO
Instituto Nacional de Tecnologías de la Comunicación

anova
Consulting Technology Innovation

Guía para el uso seguro del DNI electrónico en Internet

dni electrónico

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

Edición : Octubre 2010

El **Instituto Nacional de Tecnologías de la Comunicación** (INTECO), sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional. Para ello, INTECO desarrollará actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad, Calidad TIC y Formación.

El Observatorio de la Seguridad de la Información **(http://observatorio.inteco.es)** se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica, siendo un referente nacional e internacional al servicio de los ciudadanos, empresas, y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

Más información: **www.inteco.es**

Anova IT Consulting es una empresa española de referencia en el mercado de Consultoría de Procesos de Negocio, I+D+i, Servicios Tecnológicos y Formación.

Está especializada en el diseño, planificación y ejecución de proyectos de I+D+i relacionados con la Seguridad de la información, Video Vigilancia, Biometría, Tratamiento digital de imágenes, Borrado Seguro y Negocio electrónico, fomentando la transferencia Ciencia-Tecnología-Empresa.
Desarrolla proyectos innovadores relacionados con sistemas de movilidad, seguridad de la información, desarrollo de contenidos digitales y audiovisuales, formación especializada en TIC, outsourcing global TIC y de procesos de negocio.

Para garantizar el éxito de sus proyectos, Anova IT Consulting cuenta con un laboratorio de I+D+i y un equipo de profesionales de reconocida experiencia que trabajan en el diseño de soluciones tecnológicas novedosas que incidan eficazmente en el desarrollo integral de la sociedad. Colabora con entidades nacionales e internacionales, aportando la experiencia y el conocimiento acumulado por sus investigadores y consultores, fomentando la innovación tecnológica a partir de la transferencia del conocimiento, con la finalidad de proporcionar las mejores soluciones adaptadas a las necesidades de sus clientes, de forma eficaz y flexible.

Más información: **http://www.anovagroup.es**

Datos de contacto:
Instituto Nacional de Tecnologías de la Comunicación (INTECO)
Observatorio de la Seguridad de la Información
Avda. José Aguado, 41. Edificio INTECO. 24005 León
Teléfono: +(34) 987 877 189 / Email: observatorio@inteco.es
www.inteco.es

Depósito Legal: LE-1383-2010
Imprime: Imprenta Sorles

Índice

1. Introducción

El Documento Nacional de Identidad, DNI, es el documento oficial que confirma la identidad personal de cada ciudadano.

La apariencia de la versión electrónica del Documento Nacional de Identidad es bastante similar al DNI tradicional. La mayor diferencia que presenta el DNI electrónico es la incorporación de un chip que permite a su titular acreditarse digitalmente. Del mismo modo le permite firmar electrónicamente documentos con seguridad en las operaciones y con plena validez jurídica.

> El DNI electrónico aporta también rapidez, comodidad e inmediatez en la realización de trámites administrativos y comerciales a través de Internet.

En el marco actual, las Tecnologías de la Información ofrecen a los usuarios la opción de realizar numerosas operaciones comunes utilizando la red. Por ejemplo:

- Obtener un Certificado de Vida Laboral en pocos minutos.
- Realizar un curso e-Learning, a distancia (posibilidad de obtener títulos oficiales y Certificados)
- Reservar un libro de la biblioteca.
- Comprar un billete de avión.
- Acceder a un banco para comprobar los últimos ingresos.
- Firmar electrónicamente una factura.

Estas posibilidades han supuesto una doble ventaja para el ciudadano: no se requieren desplazamientos, ya que el titular no tiene que acudir a la entidad donde tenga que realizar el trámite, y no está sujeto a horarios, evitándose así conflictos temporales entre las actividades cotidianas del titular y las operaciones que éste tenga que realizar.

Ventajas del uso del DNIe

Debe entenderse el uso del DNI electrónico como una auténtica oportunidad para acelerar la implantación de la Sociedad de la Información en España, lo que, sin duda, influirá en beneficio de todos los ciudadanos y de la propia Administración Pública.

2. El DNI electrónico: transacciones a través de la Red

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

El DNIe[1] responde a la necesidad de facilitar la realización de operaciones telemáticas con la Administración Pública, empresas y con otros ciudadanos, proporcionando a los usuarios una mayor garantía de protección y seguridad.

Se concibe como una oportunidad para el ahorro de tiempo y recursos, sin renunciar a la privacidad. Pone al alcance del ciudadano una eficaz y avanzada herramienta que le ofrece la opción de efectuar:

- Trámites con la Administración Pública (ej. obtener la Vida Laboral).
- Trámites con empresas y otros agentes del sector privado (ej. acceder a una compañía de seguros).
- Trámites entre los ciudadanos (ej. realizar un contrato de alquiler sin necesidad de desplazamiento entre personas que están en dos ciudades diferentes).

1 A partir de ahora se utilizará la denominación de DNI electrónico y DNIe indistintamente.

2.1 NORMATIVA LEGAL

El DNIe, como el instrumento que permite la interacción física y telemática, posee, tanto en su definición como proyección, una base legal bien definida:

- **Artículo 12.1 de la Ley Orgánica 2/1986, de 13 de Marzo**, de Fuerzas y Cuerpos de Seguridad:

  "Además de las funciones comunes establecidas en el artículo anterior, se establece la siguiente distribución material de competencias: Serán ejercidas por el Cuerpo Nacional de Policía: La expedición del documento nacional de identidad y de los pasaportes."

- **Artículo 9 de la Ley Orgánica 1/1992**, de 21 de Febrero, sobre Protección de la Seguridad Ciudadana:

  "Todos los españoles tendrán derecho a que se les expida el Documento Nacional de Identidad que gozará de la protección que a los documentos públicos y oficiales otorgan las leyes y que tendrá, por sí solo, suficiente valor para la acreditación de la identidad de las personas."

  "El Documento Nacional de Identidad será obligatorio a partir de los catorce años."

URL de referencia: http://www.dnielectronico.es

- **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.

- **Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.**

- **Ley 59/2003, de 19 de Diciembre**, ley que regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

- **Artículo 1 del Real Decreto 1553/2005, de 23 de Diciembre**, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

  "El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo."

  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. […]"

- **Ley 11/2007, de 22 de Junio**, de acceso electrónico de los ciudadanos a los Servicios Públicos.

- **Artículo 2 de la Ley 56/2007, de 28 de Diciembre**, de Medidas de Impulso a la Sociedad de la Información (LISI)

  "Obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general

de especial trascendencia económica deberán facilitar a sus usuarios un medio de interlocución telemática que, mediante el uso de certificados reconocidos de firma electrónica, les permita la realización de, al menos, los siguientes trámites:

- *Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.*

- *Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere. […]"*

- **Real Decreto 1586/2009, de 16 de octubre**, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, que regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

- **Real Decreto 1671/2009, de 6 de noviembre**, que desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

- **Orden PRE/3523/2009, de 29 de diciembre**, por la que se regula el Registro Electrónico Común.

- **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.

- **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.

2.2 UTILIZACIÓN DEL DNI ELECTRÓNICO

Con el DNI electrónico son dos los aspectos que se cubren en el momento de llevar a cabo una gestión:

1. Autenticación de la identidad.

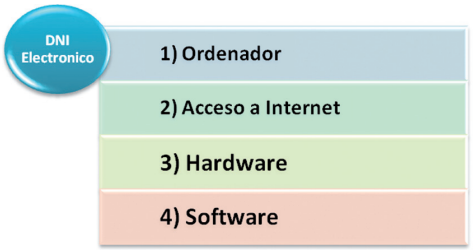
1. Firma electrónica de documentos.

Al estar realizado en policarbonato, el DNI electrónico ha mejorado notablemente su calidad, durabilidad y sobre todo su nivel de seguridad. En pocas palabras, el DNI electrónico debe utilizarse durante el proceso de realización de una transacción o actividad telemática, donde el usuario ha de identificarse introduciendo su documento en un lector de tarjetas inteligentes. Así se confirma plenamente la identidad del titular del trámite.

Para su utilización, es preciso introducir el DNI electrónico en el ordenador desde donde se van a realizar las operaciones.

Con ese objetivo se requieren los siguientes componentes:

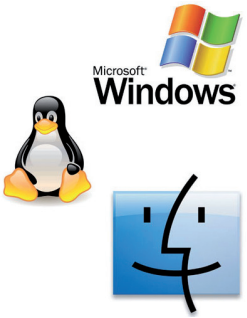
Elementos necesarios para la utilización del DNI electrónico



A continuación se ofrece una explicación detallada de cada uno de los elementos necesarios para llevar a cabo las operaciones con el DNI electrónico.

Ordenador

Los requisitos que debe cumplir el equipo informático con el que se quiere usar el DNI electrónico son básicos. Cualquier ordenador común puede ser plenamente útil. El equipo debe disponer al menos de un Microprocesador Intel -a partir de Pentium III- o tecnología similar.



El DNI Electrónico está ideado para su correcto funcionamiento en los principales Sistemas Operativos:

- Microsoft Windows (2000, XP, Vista y 7).
- Linux.
- Mac.

Acceso a Internet

Puesto que la Red va a ser el medio a través del cual se realicen las gestiones, es preciso que el ordenador tenga una correcta conexión a Internet para que la información fluya sin problemas. En sentido estricto, todo trámite en línea consiste básicamente en transmitir y recibir unos datos determinados desde un equipo a otro, utilizando la Red como medio.

Tipo de conexión a Internet

Será plenamente válida cualquier conexión. El acceso a las páginas web se realizará a través del correspondiente navegador de Internet. El DNI electrónico funciona correctamente con:

- Microsoft Internet Explorer (versión 6.0 o superior)
- Mozilla Firefox (versión 1.5 ó superior)

Hardware (lector de tarjetas inteligentes)

El DNI electrónico está desarrollado en un nuevo soporte, similar al de una tarjeta bancaria que posee un chip en la parte izquierda. Esto lo convierte en un tipo de tarjeta inteligente[2].

El DNI electrónico debe colocarse en un lector de tarjetas inteligentes. Se trata de un dispositivo diseñado para el reconocimiento de este tipo de documentos, en el que éste se introduce físicamente.

Lector tarjetas inteligentes

El lector (que debe cumplir el estándar ISO-7816[3]) debe conectarse de manera correcta a un ordenador. La tarjeta tiene que insertarse por el lado del chip, como se opera, por ejemplo, en un cajero electrónico.

2 Tarjetas de pequeño tamaño que tienen habilitado un circuito integrado que les permite realizar una serie de tareas, dependiendo de si ese circuito es de sólo memoria o dispone de un microprocesador.

3 Estándar internacional relacionado con las tarjetas electrónicas de identificación.

Existen tres tipos fundamentales de lectores: integrados en el teclado, externos (vía USB) o a través de una interfaz PCMCIA.

Integrados en el teclado

El propio teclado de un equipo puede disponer de lector. En este caso se opera válidamente con los elementos hardware que ya se poseen.

Se debe tener en cuenta que además necesitan programas informáticos (drivers) que sean capaces de interpretar adecuadamente la información del DNI electrónico. Ello obedece a que el mecanismo del teclado está diseñado para todas las tarjetas inteligentes, y el DNI electrónico tiene unas particularidades propias.

Lector de teclado

Externos

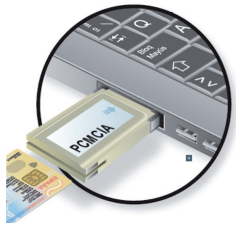
Consiste en un dispositivo que está conectado al equipo a través del puerto USB (Puerto Serie Universal). Otros elementos externos habituales pueden ser una impresora, pendrive de memoria, etc.

Lector periférico

Interfaz PCMCIA

Este tipo de dispositivo se inserta en el puerto PCMCIA de los ordenadores portátiles, permitiendo la lectura del DNI electrónico en el equipo al introducir el documento en la tarjeta lectora.

Interfaz PCMCIA



Software

El software necesario para operar con el DNI electrónico es imprescindible para que el documento funcione correctamente y permita al ciudadano realizar trámites de manera cómoda. A continuación se expone el software que permite que el ordenador pueda operar adecuadamente con el lector de tarjetas.

Controladores

Los controladores también se denominan *drivers*. Son programas necesarios para que el ordenador consiga reconocer el lector de tarjetas inteligentes y poder intercambiar información.

Selección de módulos y controladores en el proceso de instalación

Ante un lector de tarjetas periférico, el ordenador puede no ser capaz de comunicarse con él. En este caso se instalan los controladores (por regla general serán suministrados por el fabricante y acompañarán al lector). No obstante, la mayoría de sistemas operativos los incorporan por defecto.

Módulos criptográficos

Además, para que el chip de la tarjeta sea reconocido adecuadamente, el equipo debe tener incorporado otro tipo de programas. Son los módulos criptográficos.

Si se pretende trabajar bajo un Sistema Operativo Microsoft Windows, el equipo debe tener instalado un servicio denominado Cryptographic Service Provider (CSP). Si, en cambio, se tienen otros entornos (UNIX / Linux o MAC) para utilizar el DNI electrónico, es necesario poseer el módulo criptográfico denominado PKCS#11.

URL de descargas del módulo criptográfico

La descarga gratuita de estos módulos es posible a través de la url: **www.dnielectronico.es/descargas/**

3. Protección del DNI electrónico frente a los ataques informáticos

El DNIe aporta rapidez, comodidad, la inmediata realización de trámites administrativos y comerciales a través de medios telemáticos, pero ante todo aporta **seguridad**.

Se trata de una herramienta que contiene una "llave" para que cómodamente se puedan realizar también trámites a través de la Red. Utilizarlo correctamente, como cualquier "llave", proporciona un entorno de comunicación y gestión enormemente seguro.

3.1 FORMATO

El DNIe se compone de una tarjeta de policarbonato, a la que se han añadido diferentes elementos de seguridad contra la falsificación (hologramas, letras táctiles, imágenes múltiples a láser, tintas fluorescentes [UV/I], tintas que cambian de color [OVID], imágenes codificadas, microtextos, kinegramas, etc.) e incorpora un chip criptográfico.

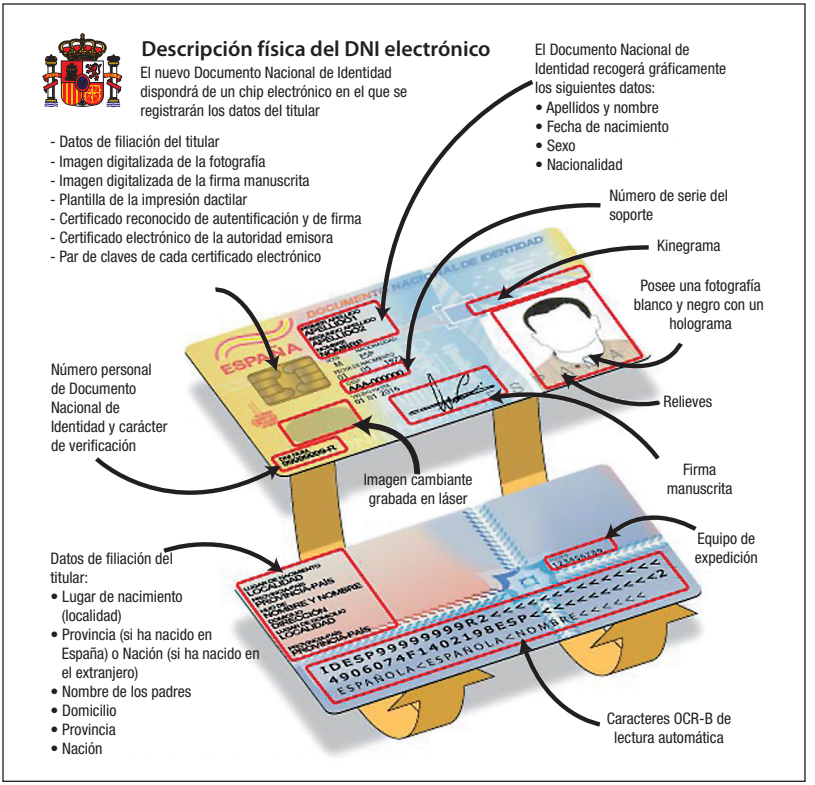
La realización del DNIe en policarbonato obstaculiza su falsificación y la incorporación del chip multiplica exponencialmente su seguridad.

El microchip, que constituye la principal novedad visible por el usuario, almacena la siguiente información:

- Certificado electrónico para autentificar al ciudadano.
- Certificado electrónico para poder firmar electrónicamente.
- Certificado de la Autoridad de Certificación emisora (DNI electrónico).
- Claves para su utilización (PIN).

- Huella dactilar (se almacenan los rasgos característicos de la huella digitalizada).
- Fotografía digitalizada.
- Firma manuscrita en formato digital.
- Datos básicos que aparecen escritos

Descripción física del DNI electrónico



3.2 FUNCIONAMIENTO

El objetivo del DNI electrónico es dotar de mayor seguridad a los trámites que se pueden llevar a cabo a través de Internet. Con este fin se encuentran los mecanismos que priorizan la máxima privacidad y garantía del sistema.

Cuadro resumen mecanismos para la seguridad del sistema

El código PIN (Personal Identification Number)

Es un código de seguridad que funciona de forma similar al de un teléfono móvil o una tarjeta bancaria. Es decir, impide que cualquier otra persona que no sea el legítimo titular (que conoce el PIN) pueda utilizar el DNIe a través de Internet para identificarse y firmar digitalmente.

Ventana de Windows para introducir el PIN del DNIe

Siempre que se pretenda realizar algún trámite electrónico, será necesario acreditar la identificación previamente, introduciendo la clave de seguridad (el número PIN).

Sin el PIN no es posible realizar ningún tipo de operación telemática. Esto asegura que sea el titular del DNI electrónico quien pueda acceder y realizar operaciones telemáticas a través de Internet de manera exclusiva. Por su propia relevancia, más adelante se hablará con más profundidad de este código, su modificación y comprobación.

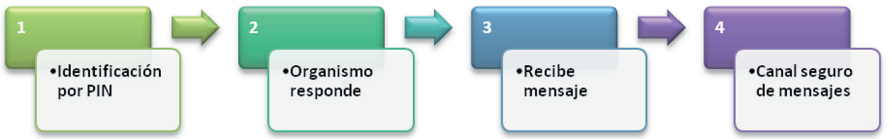
Acceso seguro

El uso del DNI electrónico incorpora nuevos avances tecnológicos para evitar cualquier posible ataque de terceras personas. Es un procedimiento de conexión que confirma en todo caso que el ciudadano autentificado con el PIN realiza de manera segura los trámites.

El protocolo de uso del DNIe contempla el siguiente esquema, una vez que el ciudadano conecta con el Organismo Público o Entidad Privada (por ejemplo con la página web de la Agencia Tributaria, o la de un determinado banco). El proceso se puede resumir en:

1. El ciudadano solicita el trámite y se identifica con su PIN.
2. El Organismo responde al ciudadano y le envía un mensaje.
3. El ciudadano recibe el mensaje para confirmar su deseo de solicitar ese trámite.
4. Se establece un canal seguro de mensajes.

Proceso de conexión segura del ciudadano con una entidad



Solicitar la vida laboral ante la Tesorería General de la Seguridad Social a través de Internet.

Se accede a la web de la Tesorería.Se introduce el DNI electrónico en el lector y se confirma la identidad del interesado marcando el PIN.

La Tesorería lee la información del chip, reconociendo así la personalidad del ciudadano (establece que una determinada persona, con nombre y apellidos, está solicitando un trámite concreto a través de Internet).

La Tesorería envía un mensaje indicando que ha reconocido al particular, permitiéndole acceder a sus servicios a través de la Red.

Se crea para ello un canal seguro, SSL (Secure Socket Layer).

Páginas seguras

Las gestiones que se realizan con el DNI electrónico en la Red se realizan en páginas web seguras, es decir, aquellas webs que tienen un protocolo específico de seguridad, para garantizar la adecuada interacción del DNI electrónico.

En estas páginas web se advierten relevantes diferencias. Una de las diferencias más importantes es el tipo de protocolo que utilizan (http o https). Visualmente se diferencian por empezar con https en lugar de http (la s final significa *secure*) y por un candado cerrado o una llave que aparece en la parte inferior del navegador. Mediante el protocolo seguro https la transmisión se hace cifrada a diferencia del protocolo http, en el que la transmisión se realiza en claro.

Barras del explorador de una página web segura en Mozilla Firefox e Internet Explorer

4. Autentificación y firma electrónica

Los principales activos que se encuentran en la utilización del DNI electrónico en entornos digitales consisten en la posibilidad de realizar gestiones telemáticas desde cualquier lugar y a cualquier hora del día.

El DNIe ofrece al usuario dos posibilidades o funcionalidades complementarias. Ambas opciones se encuentran incorporadas en el certificado electrónico que reside dentro del chip. Estas alternativas son: la autentificación y la firma electrónica.

Operaciones básicas que permite el DNI electrónico

4.1 AUTENTIFICACIÓN

Mediante la autentificación, un individuo en una determinada operación, es capaz de identificarse de manera irrefutable.

Para identificarse de manera telemática son requeridas una serie de medidas. El DNIe, además de la capacidad de identificación física de su titular, posee la funcionalidad para identificar al ciudadano en medios digitales. De esta manera se evita la suplantación de personalidad.

> *Por ejemplo, al solicitar a través de Internet un certificado de antecedentes penales, la autentificación correcta confirma que el referido certificado de penales lo está pidiendo el interesado, no cualquier otra persona.*

Dicho de otro modo, cuando se accede a determinados sitios de Internet, es preciso demostrar incuestionablemente que una determinada persona es precisamente esa quien dice ser. Esto es factible de validar formalmente accediendo con un DNI electrónico y confirmándolo con el PIN.

4.2 FIRMA ELECTRÓNICA

La firma electrónica es el conjunto de datos digitales, que pueden asegurar que se ha firmado un determinado trámite o documento. De esta manera se acredita que la persona que ha firmado está plenamente de acuerdo con ese trámite o documento en particular.

La firma electrónica identifica al firmante de forma única igual que su firma manuscrita. Es posible verificar que los documentos firmados no hayan sido alterados por terceras partes y un documento firmado electrónicamente no puede repudiarse por parte de su firmante.

Programa para firmar electrónicamente

La legislación (Ley 59/2003, de 19 de diciembre, de firma electrónica) distingue entre dos tipos de firma electrónica:

1. **Firma electrónica avanzada:** (Art. 3.2) 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.

2. **Firma electrónica reconocida:** (Art. 3.3) firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. (Art. 3.4) La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los datos consignados en papel.

Funcionamiento de la Firma Electrónica

Con los datos que existen en el DNIe (certificado de firma) y el fichero a firmar, un programa crea el código necesario que luego acompaña al documento o trámite, y que tiene el mismo valor legal que si se hiciera en papel. Desde un punto de vista técnico, se sigue el siguiente proceso:

1. Se establece la conexión del ciudadano provisto de su DNI electrónico con la Entidad Pública o con una Entidad Privada.

2. El ciudadano se autentifica (se reconoce formalmente que él es la persona que dice ser).

3. Se establece un canal seguro de comunicación.

Proceso de comunicación seguro

En el protocolo de construcción de este canal seguro de comunicación, intervienen varios protagonistas:

- **Certificado de Organismo Público (o Entidad Privada).**

  Este certificado asociado al servidor del Organismo o Entidad, garantiza que el ciudadano se está conectando a dicha entidad y no a cualquier otra.

- **Certificado de autenticación del ciudadano.**

  El ciudadano para identificarse frente al Organismo (o Entidad Privada) requiere un certificado con capacidad de autenticación. De esta manera el anterior Organismo podrá reconocer la identidad del ciudadano. La validez de este certificado viene determinada por la Dirección General de la Policía. Este certificado, como ya se ha mencionado anteriormente, se encuentra incorporado en el DNI electrónico.

Protocolo para firmar electrónicamente un trámite

Los pasos a seguir para firmar electrónicamente un trámite son los siguientes:

1. El Organismo Público (o Entidad Privada) muestra un formulario para el trámite determinado.

2. El ciudadano cumplimenta el formulario y lo acepta.

3. El Organismo Público (o Entidad Privada) reconstruye el formulario en formato texto y lo reenvía nuevamente al ciudadano, para su comprobación.

4. El ciudadano comprueba que el trámite que está solicitando es exactamente el que pretende (por ejemplo solicitud de subvención).

5. Se pide que el ciudadano firme electrónicamente.

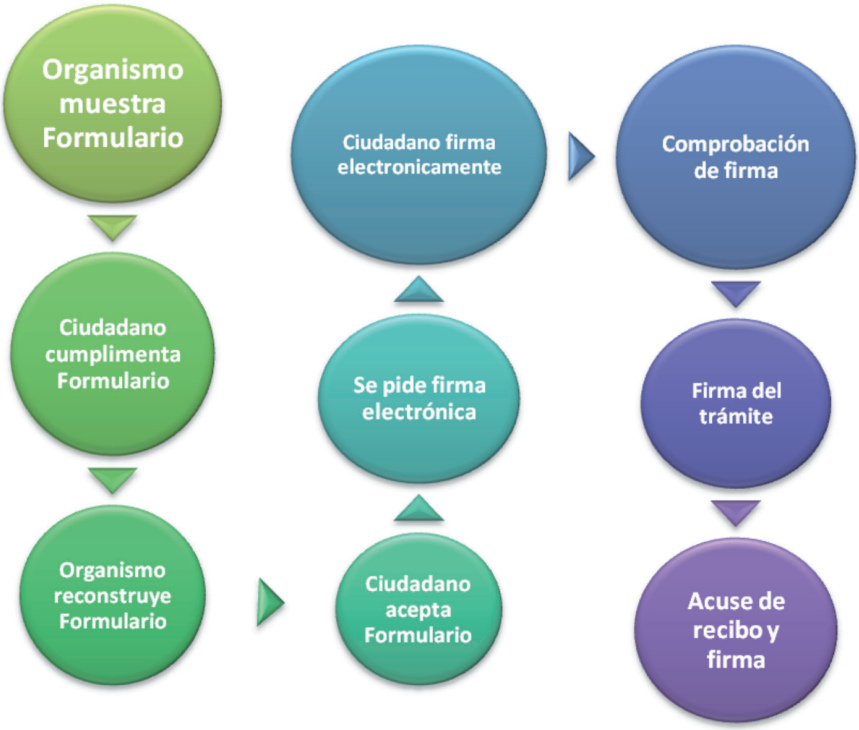
6. El ciudadano, con su PIN y DNIe, procede a firmar el trámite.

7. El Organismo Público (o Entidad Privada) comprueba que la firma es correcta y que el Certificado electrónico está activo.

8. Se procede a la firma electrónica del trámite.

9. El Organismo Público (o Entidad Privada) entrega al ciudadano un formulario donde consta el acuse de recibo y la firma.

Protocolo seguro de firma electrónica



5. Código PIN

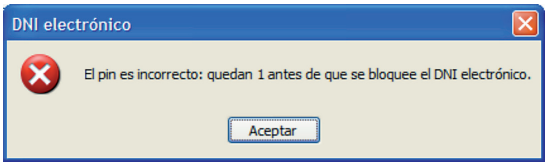
Como se adelantó en el epígrafe 3, consiste en una **clave secreta**, (como la de una tarjeta bancaria o la de un teléfono móvil) que tiene por objetivo impedir que nadie que no sea su legítimo titular, pueda utilizar un DNI electrónico ajeno.

Si no se introduce el PIN no se podrá realizar ninguna operación a través de Internet ni en ningún otro caso. El PIN constituye la "llave" que posibilita acceder al mundo virtual con un DNI electrónico.

PIN como código personal de seguridad

Como si se tratara de un teléfono móvil y para reforzar la seguridad, el hecho de introducir incorrectamente el código 3 veces consecutivas, conllevará el bloqueo del PIN imposibilitando la acción de operar en la Red con el mismo. Para desbloquearlo será preciso acudir a las Oficinas de Expedición del DNIe (en algunas ciudades estas oficinas se encuentran en las Comisarías de Policía).

Alerta al introducir un PIN incorrecto

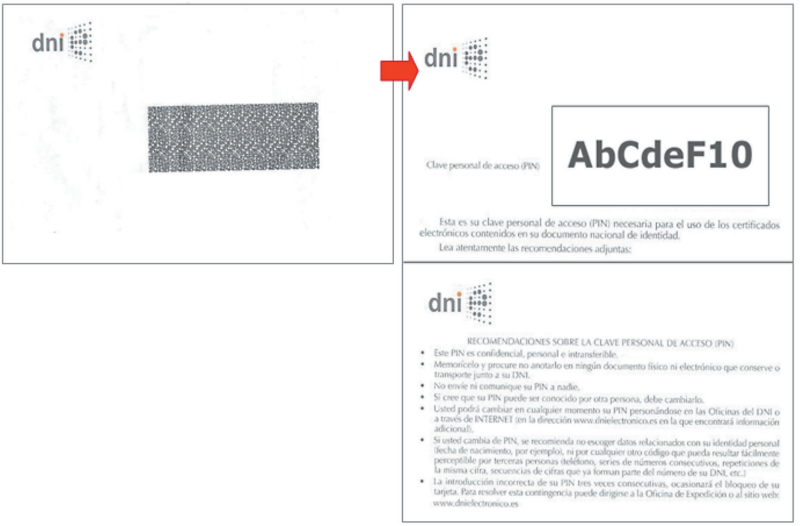


5.1 OBTENCIÓN DEL CÓDIGO PIN

En el momento de la expedición del DNIe, se genera un PIN aleatorio de **8 a 16 dígitos** de **carácter alfanumérico** (puede incorporar letras y/o números. Se distinguen mayúsculas y minúsculas) que se entrega al ciudadano en un sobre cerrado.

A partir de su obtención es importante recordar que el PIN es la contraseña que salvaguarda las claves privadas del usuario y, por tanto, es privado, personal e intransferible.

Exterior e interior del sobre que contiene el PIN original



Debido a que el código original es generado aleatoriamente, es inconexo o de difícil memorización para el usuario.

El objetivo es que el ciudadano pueda conocer el PIN en cualquier momento y lugar (cuando surja la necesidad de realizar algún trámite que lo precise). Por ello puede ser aconsejable no tenerlo anotado en el sobre original, en algún otro papel o en un documento digital, siendo recomendable que se proceda a modificar el PIN inicial por otro código que sea más cómodo de memorizar.

5.2 MODIFICACIÓN DEL CÓDIGO PIN

El protocolo para modificar el PIN es muy sencillo. Existen dos alternativas:

- Modificación del código PIN a través de Internet.
- Modificación del PIN personándose en una Oficina de Expedición del DNI.

Modificación del código PIN a través de Internet

Es necesario acudir a la web habilitada que permita hacerlo. Se trata de una sección dentro de la página creada por el Cuerpo Nacional de Policía expresamente sobre DNI electrónico que permite la modificación del código PIN.

Aquí se indica el proceso a llevar a cabo para asegurar la correcta modificación de la clave. El cambio no se produce directamente en la página web, introduciendo los datos.

Ventana para ejecutar el PAD

Es preciso descargar un software específico denominado PAD[6] (Punto de Actualización del DNIe virtual).

Una vez que se realice la descarga, será preciso instalar el programa desde donde se podrá efectuar el cambio de PIN. Para máxima seguridad, es requisito imprescindible conocer el PIN actual para modificarlo por otro. Si se desconoce este, el usuario sólo podrá cambiarlo personalmente en un Punto de Actualización del DNIe, ubicado en una Oficina de Expedición.

Modificación del PIN personándose en una Oficina de Expedición del DNI

En este caso, el ciudadano debe acudir a un Punto de Actualización del DNIe (PAD), ubicado sólo en aquellas oficinas[7] que expendan el DNI electrónico.

Quiosco PAD. Punto Actualización DNI

En estos Puntos de Actualización se puede introducir el DNIe en la ranura y tras teclear el código PIN para identificarse se puede proceder a la modificación del mismo. En caso de que se desconozca el PIN, o haya sido bloqueado por

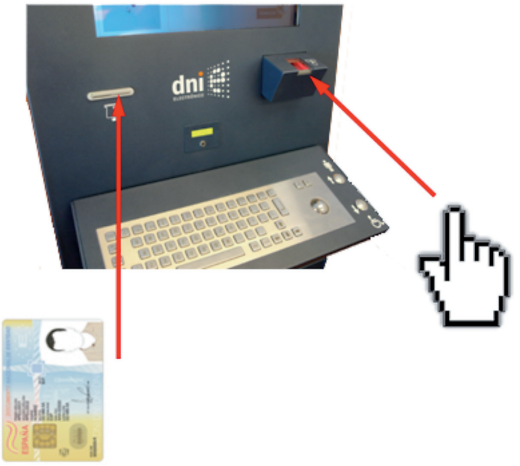
6 http://www.dnielectronico.es/descargas/kiosko_virtual.html

7 http://www.policia.es/udoc/dni/mapa_oficinas.htm

introducirlo erróneamente tres veces, en estos Puntos de Actualización se encuentra un lector de huella dactilar, que permite comparar la información criptográfica de la huella dactilar del titular con la que se almacena en el chip en el momento de la expedición.

Cuando el reconocimiento es validado, la aplicación permite al titular cambiar el PIN de su DNI electrónico.

Funcionamiento del PAD



Los Puntos de Actualización del DNI permiten tres trámites diferentes:

- Modificación del PIN.
- Desbloqueo del PIN, si fue anteriormente bloqueado al introducir 3 intentos incorrectos de manera sucesiva.
- Renovación del Certificado electrónico.

Por motivos de seguridad el Certificado electrónico caduca a los 30 meses. Desde un mes antes de su caducidad, es posible renovarlo por otros 30 meses más.

Es obligatorio llevar a cabo el trámite de la renovación del Certificado en los PAD de las oficinas de expedición. No es posible hacerlo a través de Internet. Un Certificado electrónico caducado no supone que el DNI electrónico lo esté, aunque imposibilita que se pueda realizar trámites a través de Internet.

Para comprobar que el DNIe funciona y que el los certificados electrónicos están activos, en un ordenador, una vez insertado el DNI electrónico en el lector, se puede acudir a la sección del Portal Oficial sobre el DNI electrónico y acceder a su área de descargas, para instalar el software adecuado en función del sistema operativo que se esté usando.

Comprobación del Certificado Autenticación de su DNIe

COMPROBACIÓN DEL CERTIFICADO DE AUTENTICACIÓN DE SU DNI ELECTRÓNICO

Estimado Sr/Sra. ##############

Su DNIe acaba de ser verificado. Esta usted en disposición de un Certificado de **Autenticación Activo**.

Identificador	Valor
INFORMACIÓN SOBRE LA IDENTIDAD	**(Valores Personales)**
Nombre	###### (AUTENTICACIÓN)
Apellidos	##############
NIF	#########
Número de Serie del Certificado de Autenticación	############## ########################## ##########################
Autoridad Emisora	AC DNIE 002
Propietario	############ ################## ##################
Comienzo de la Validez del Certificado	############
Fin de la Validez del Certificado	25 de septiembre de 2010
Estado del Certificado de Autenticación	Activo

Si todo funciona adecuadamente, tras haber introducido el PIN la aplicación leerá el Certificado del DNI electrónico y mostrará esta ventana.

6. DNI electrónico. Garantía de identidad

6.1 GARANTÍA DE IDENTIDAD DE LA FIRMA ELECTRÓNICA

Como se ha comentado con anterioridad, el chip electrónico que posee el nuevo DNI electrónico contiene la información relativa a la identidad personal del titular, por lo que se ha hecho mucho hincapié en subrayar que se cumplen las necesidades de privacidad.

En este capítulo se recopila y recalca lo más significativo de cara a transmitir tranquilidad y seguridad a los usuarios de las funcionalidades que el DNI electrónico ofrece.

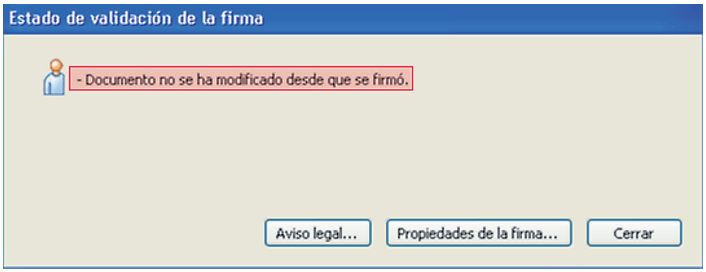
Esta seguridad se encuentra no sólo referida a la firma electrónica, sino a los tres aspectos que contempla:

1. **Acreditación de la identidad.** El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice ser. El ciudadano podrá además acreditar su identidad frente a una tercera persona.

2. **Instrumento para firmar electrónicamente un documento.** Mediante la utilización del Certificado de Firma (*nonRepudiation*), la persona que recibe un mensaje firmado electrónicamente puede verificar que la firma es correcta y que el firmante no puede repudiarlo.

3. **Certificación de la integridad de un documento.** El Certificado también hace posible comprobar que un determinado documento no ha sido modificado. Esto se produce mediante la utilización de funciones resumen (*hash*) y la encriptación del mensaje y la firma electrónica. Si se rectifica el documento, se indicará que éste ha sido alterado.

Mensaje de aplicación informática confirmando la integridad del documento



Esta identidad de la persona física que está utilizando el DNIe queda fehacientemente acreditada en varios niveles:

Autentificación mediante PIN

El DNI electrónico solicita el PIN que procederá al autobloqueo al realizar tres intentos incorrectos (CHV[9]- *Card Holder Verification*). El código PIN es personal e intransferible. Únicamente debe ser conocido por el propio titular del documento.

Autentificación de aplicación

Su objetivo es que la aplicación en la que se desarrolla un trámite, demuestre conocer un determinado nombre y un código, para aumentar la seguridad y mostrar que realmente se está frente a la entidad que solicita el trámite. Se siguen estos pasos.

---

9 Verificación del titular del DNIe. Esta operación se lleva a cabo comprobando el código facilitado por la entidad externa a través del correspondiente comando. Cada código tiene su propio contador de intentos. Éste decrece cada vez que se realiza una introdución errónea.

- La aplicación pide un desafío a la tarjeta.
- La aplicación debe emplear un algoritmo a este desafío junto con el correspondiente código secreto y nombre de la clave.
- La tarjeta realiza la misma operación y compara el resultado con los datos transmitidos por la aplicación. En caso de coincidir, considera correcta la presentación para posteriores operaciones.

Autentificación mutua

Para garantizar plena confianza entre las dos partes de una operación (usuario y entidad).

> En el proceso de autenticación mutua, también se incluye el intercambio seguro de unas claves de sesión, que deberán ser utilizadas para securizar (cifrar) todos los mensajes intercambiados posteriormente. Este servicio permite el uso de diferentes alternativas.

Las dos opciones disponibles están basadas en la especificación *'CWA 14890-1 Application Interface for smart cards used as Secured Signature Creation Devices – Part 1'*[10], y son las siguientes:

- Autenticación con intercambio de claves (descrita en el capítulo 8.4 de CWA 14890-1).
- Autenticación de dispositivos con protección de la privacidad, (descrita en el capítulo 8.5 de CWA 14890-1).

10 Estándar de firma electrónica

Seguridad de los mensajes

La tarjeta permite la posibilidad de establecer un canal seguro para confirmar el contenido de los mensajes (HTTPS). El canal seguro nos permite conocer la identidad de las partes, y la comunicación entre ambas está cifrada para asegurar que nadie ajeno a ella pueda acceder a su contenido.

6.2 SOFTWARE PARA LA FIRMA ELECTRÓNICA

Para hacer trámites utilizando todo el alcance de la firma electrónica, a veces puede ser necesario disponer de un determinado software que genere la propia firma electrónica.

> ***Firma electrónicamente un contrato de alquiler de una plaza de garaje posteriormente a su redacción.***
>
> *Existen numerosas formas de hacerlo:*
>
> *1) Es factible elaborar en cualquier procesador de texto el contrato de alquiler de la plaza de garaje y luego con el mismo procesador, obtener la opción de firmarlo electrónicamente.*
>
> *2) También se puede hacer uso de programas que permitan incorporar la firma al documento digital del contrato de alquiler.*

Programas para la firma electrónica de documentos

Existe una amplia relación de ellos, y muchos son de carácter libre. Algunos no sólo permiten firmar electrónicamente documentos de texto, sino también cualquier otro tipo de archivos (por ejemplo firmar una imagen donde quede reflejada la fecha y el autor de la misma). Entre algunas opciones podemos encontrar:

- **Aplicación firma del Ministerio de Industria, Turismo y Comercio (eCoFirma)**

www.inteco.es/Seguridad/DNI_Electronico/Firma_Electronica_de_Documentos

- **@firma. Plataforma de validación y firma electrónica**

www.csae.map.es/csi/pg5a12.htm

6.3 PRIVACIDAD

Desde su concepción originaria, se ha incidido en la necesidad de que el DNI electrónico haga un esfuerzo por preservar la privacidad de los usuarios. Como el DNI anterior se incluyen en la tarjeta los mismos datos autorizados hasta la fecha (nombre, domicilio, fecha de nacimiento, etc.). El DNI electrónico no persigue controlar al ciudadano ni almacenar datos de acceso a Internet, preferencias o información de cualquier otra índole.

Esto está estipulado y regulado por la ley orgánica de protección de datos (LOPD), encargada de establecer una serie de requisitos que garantizan el escrupuloso respeto a los derechos de los ciudadanos de privacidad e intimidad. Estas exigencias, las cumple de forma estricta y en todo momento el nuevo DNI electrónico.

Sólo se va a tener acceso a los datos que se incluyen en el DNI desde la dirección general de policía y de la guardia civil y fuerzas de seguridad del estado y autonómicas, y únicamente para requisitorias de identificación de los distintos cuerpos policiales.

Protocolo de privacidad

En todo momento el ciudadano debe tener garantizada su privacidad, tanto frente a los Poderes Públicos, como frente a otros ciudadanos. En este último sentido se encuentran determinados instrumentos para garantizarlo.

El PIN juega un papel primordial, su uso adecuado confirma que no pueda acceder cualquier otra persona diferente del propio titular. Por ese motivo, en caso de que el interesado pueda creer que algún otro ha podido identificar su PIN, sería preciso proceder a su modificación, por cualquiera de las vías disponibles que se han comentado en el capítulo anterior.

7. Enlaces de interés

Si el usuario está interesado en conocer más acerca del DNI electrónico, a continuación se expone una serie de direcciones web con información referida al DNIe:

- http://www.dnielectronico.es/
- http://www.usatudni.es/
- http://www.formaciondnie.es/
- http://www.inteco.es/Seguridad/DNI_Electronico/

¿Quieres seguirnos?

en la web: http://observatorio.inteco.es

en Twitter: @ObservaINTECO

¿Quieres hacernos llegar algún comentario?

observatorio@inteco.es

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

anova
Consulting Technology Innovation