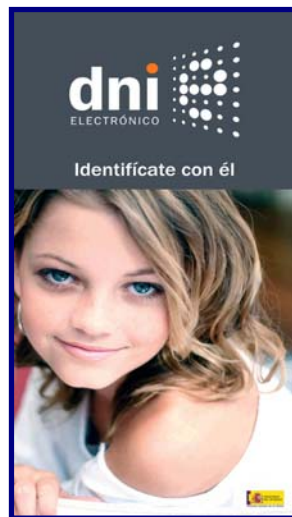
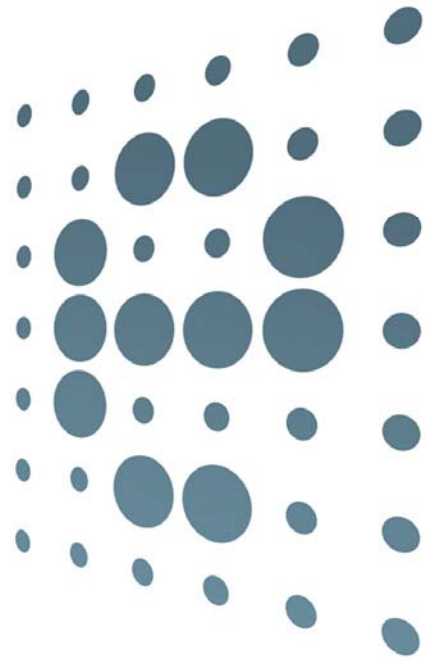


dni

electrónico



no contiene ningún otro dato del titular relativa a datos personales diferentes a los actuales ni de cualquier otro tipo (sanitarios, fiscales, de tráfico, etc.).

5.1. ¿Qué son los certificados electrónicos?

Son el conjunto de datos incluidos en el chip, que permiten la identificación de su titular (Certificado de Autenticación) y la firma electrónica de documentos (Certificado de Firma). Los datos se alojan en dos partes del chip de la tarjeta: pública y privada. La primera contiene los datos básicos de los certificados y una clave pública, mientras que la parte privada contiene la clave privada de la tarjeta, sólo conocida por su titular.

6.1. ¿Para qué sirven los certificados?

El certificado de Autenticación sirve para identificar al titular de la tarjeta en una comunicación telemática. El certificado de Firma garantiza la integridad del documento firmado, la procedencia del documento y la autenticidad de origen.

7.1. ¿Quién emite los certificados del DNI electrónico?

La Dirección General de la Policía es el único organismo autorizado a emitir los certificados digitales para el DNI electrónico. Los procedimientos de solicitud, revocación, renovación y período de vigencia de los certificados están regulados en la Política de Certificación.



2. ¿cómo será su uso?

2.1. ¿Cuáles son sus posibles usos?

El número de usos posibles enorme. En principio la utilización del DNI electrónico es válida para todo tipo de tramitación telemática: desde solicitar una beca a presentar la Declaración de la Renta y otros impuestos o acceder a los datos de la Seguridad Social, así como el acceso a información personal en bases de datos públicas, la realización de transacciones con empresas, etc.

2.2. ¿Tiene la misma validez que el tradicional?

Sí. De acuerdo con la regulación, "todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos".



2.3. ¿Cuándo será obligatorio su uso?

En cuanto a los documentos actuales y los que sean emitidos antes de la puesta en marcha del DNI electrónico, seguirán siendo válidos hasta que culmine el futuro plan de sustitución de los mismos.

2.4. ¿Cómo se usa electrónicamente el DNI?

El usuario se conecta al servidor web de un prestador de servicios (Administración pública, empresa, etc.), quien le presenta su certificado (para comprobar que se ha conectado con quien desea hacerlo) y le indica que la conexión es segura. El terminal del usuario y el servidor web se intercambian las claves públicas para iniciar una comunicación segura. Cuando el servidor web requiera de la firma electrónica del usuario, éste accederá a su certificado de firma a través de la clave privada y cumplimentará los datos solicitados por el servidor. Tras la comprobación del contenido del documento, lo firma digitalmente. A continuación se envía el documento, la firma y el certificado del usuario al prestador de servicios, quien, a través del Servicio de Validación, comprueba que los certificados no han sido suspendidos ni revocados.

2.5. ¿Cómo se obtienen las claves del DNI electrónico?

La generación de claves se realiza dentro de la tarjeta criptográfica y en presencia de su titular.

2.6. ¿Se pueden cambiar las claves del DNI electrónico?

El PIN es la contraseña que protege sus claves privadas y permite activarlas en las aplicaciones que generan firma electrónica. El PIN, que originalmente se entrega en un sobre ciego, puede ser cambiado por otro de la elección del ciudadano.

2.7. ¿Qué se debe hacer en caso de robo del DNI electrónico o si se sospecha que alguien puede haber utilizado nuestras claves?

Resulta obligado informar de manera inmediata al órgano competente para la expedición y gestión del DNI electrónico cuando exista alguna de las causas de revocación de la vigencia de los certificados (como sustracción o pérdida de la tarjeta). Así se podrán revocar los certificados comprometidos y evitar su uso ilegítimo por un tercero no autorizado.

3. ventajas del dni electrónico

Desde el punto de vista de la SEGURIDAD:

El DNI electrónico es un documento más seguro que el tradicional, pues incorpora mayores y más sofisticadas medidas de seguridad que harán virtualmente imposible su falsificación.

Mediante el DNI electrónico podremos garantizar la identidad de los interlocutores de una comunicación telemática, ya sea para intercambio de información, acceso a datos o acciones o compra por Internet. Igualmente, gestionar mejor el acceso a nuestro espacio de trabajo, nuestro ordenador personal y a la información que contenga.

Gracias al DNI electrónico podemos intercambiar mensajes con la certeza de que nuestro interlocutor es quien dice ser y que la información intercambiada no ha sido alterada.

Desde el punto de vista de la COMODIDAD:

Con el DNI electrónico se podrán realizar trámites a distancia y en cualquier momento: El DNI electrónico permitirá realizar multitud de trámites sin tener que acudir a las oficinas de la Administración y sin tener que guardar colas. Y hacerlo en cualquier momento (24 horas al día, 7 días a la semana).

El DNI electrónico se expedirá de forma inmediata: no será necesario acudir dos veces a la Oficina de Expedición, sino que la solicitud y la obtención del documento se hará en una única comparecencia, en cualquiera de las Oficinas de

Expedición existentes en España, que se irán dotando progresivamente del equipamiento necesario para la expedición del nuevo documento.

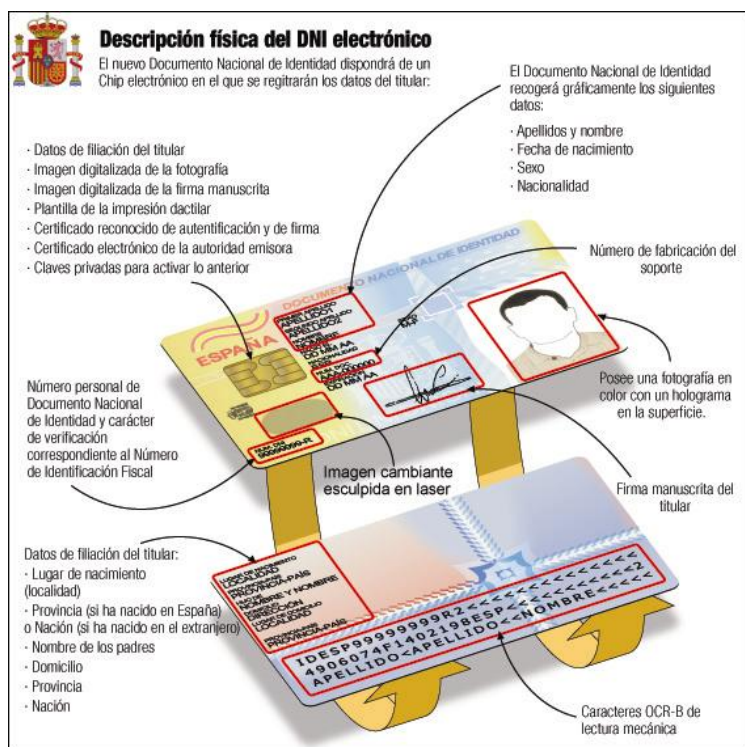
Hacer trámites sin tener que aportar una documentación que ya exista en la Administración: Una de las ventajas derivadas del uso del DNI electrónico y de los servicios de Administración Electrónica basados en él será la práctica eliminación del papel en la tramitación. El ciudadano no tendrá que aportar una información que ya exista en otra Unidad de la Administración, evitándose -de nuevo- colas y pérdidas de tiempo. La Unidad que realice la tramitación lo hará por él, siempre que el ciudadano así lo autorice.

Desde el punto de vista de la ERGONOMÍA:

El DNI electrónico es un documento más robusto. Está construido en policarbonato y tiene una duración prevista de unos diez años.

El DNI electrónico mantiene las medidas del DNI tradicional (idénticas a las tarjetas de crédito habituales).

4. descripción del dni electrónico



El DNI electrónico es una tarjeta de un material plástico (concretamente policarbonato), que incorpora un chip con información digital y que tiene unas dimensiones idénticas a las del DNI tradicional. Su tamaño, por tanto, coincide con las dimensiones de las tarjetas de crédito comúnmente utilizadas (85,60 mm de ancho X 53,98 mm de alto).

En el anverso de la tarjeta se encuentran los siguientes elementos:

- Primer apellido del ciudadano
- Segundo apellido del ciudadano
- Nombre del ciudadano
- Sexo y nacionalidad del ciudadano
- Fecha de nacimiento del ciudadano
- Número de serie del soporte físico de la tarjeta
- Fecha de validez del documento
- Número del Documento Nacional de Identidad del Ciudadano y letra
- La fecha de expedición en formato DDMMAA

- La primera consonante del primer apellido + primera consonante del segundo apellido + primera consonante del nombre (del primer nombre en caso de ser compuesto)
- Chip criptográfico , que contiene la siguiente información en formato digital:
 - Un certificado electrónico para autenticar la personalidad del ciudadano
 - Un certificado electrónico para firmar electrónicamente, con la misma validez jurídica que la firma manuscrita
 - Certificado de la Autoridad de Certificación emisora
 - Claves para su utilización
 - La plantilla biométrica de la impresión dactilar
 - La fotografía digitalizada del ciudadano
 - La imagen digitalizada de la firma manuscrita
 - Datos de la filiación del ciudadano

Elementos de seguridad del documento, para impedir su falsificación:

1. Medidas de seguridad físicas:

- Visibles a simple vista (tintas ópticamente variables, relieves, fondos de seguridad)
- Verificables mediante medios ópticos y electrónicos (tintas visibles con luz ultravioleta, microescrituras)

2. Medidas de seguridad digitales:

- Encriptación de los datos del chip
- Acceso a la funcionalidad del DNI electrónico mediante clave personal de acceso (PIN)
- Las claves nunca abandonan el chip

- La Autoridad de Certificación es el la Dirección General de la Policía

El reverso de la tarjeta contiene los siguientes elementos:

- LUGAR DE NACIMIENTO
- PROVINCIA-PAÍS
- HIJO DE
- DOMICILIO
- LUGAR DE DOMICILIO
- PROVINCIA-PAÍS y EQUIPO
- Información impresa OCR-B para lectura mecanizada sobre la identidad del ciudadano según normativa OACI para documentos de viaje.

5. la seguridad del documento

La tarjeta electrónica

El chip del DNI electrónico, presenta las siguientes características:

- Chip ST19WL34
- Sistema operativo DNIE v1.1
- Capacidad de 32K.

La estructura de los ficheros que contiene el chip del DNI seguirán el estándar PKCS#15, según la siguiente clasificación:

- Zona pública: accesible sin restricciones, contiene:
 - Claves Públicas del ciudadano
 - Certificado de la Aut. de Certificación de Producción
- Zona privada: accesible por password o mediante datos biométricos, conteniendo:
 - Claves privadas del ciudadano
 - Certificado de identidad del ciudadano
 - Certificado de firma
- Zona de seguridad: accesible por el ciudadano mediante su clave de acceso personal (PIN) y procedimiento de acceso a disposición de la Administración, en la que se encuentran los siguientes datos:
 - Datos biométricos
 - Datos de filiación del ciudadano (los mismos que están impresos en la tarjeta)
 - Número de serie del soporte.

En lo referente a las condiciones de acceso a los datos contenidos en el chip, no pueden ser modificados después de la personalización, con la única excepción de

los implicados en la renovación de los certificados. Las claves RSA no pueden leerse ni escribirse directamente, ni ser extraídas de la tarjeta, por lo que la firma electrónica se realiza únicamente en el interior de la tarjeta. . La tarjeta del DNI electrónico se constituye entonces como un dispositivo seguro de creación de firma de tipo 3 según lo establecido en la CWA-14169, es decir, el objeto de evaluación debe comprender todo el hardware implicado en el proceso, el sistema operativo (SO), la generación de los datos de Creación de Firma y los de Verificación, el almacenamiento y uso de los Datos de Creación de Firma y la funcionalidad de la Creación de la Firma. Las claves asociadas a los Certificados de Autenticación y Firma (no repudio) siempre se generaran dentro de la Tarjeta, no pudiendo las Claves Privadas abandonarla nunca. El algoritmo de comprobación de huella y el patrón de huella sólo pueden ser utilizados por la propia tarjeta.

Certificados electrónicos que contiene el chip.

- Certificado Convencional X509 de identificación de componente. El propósito de este certificado es la autenticación de la tarjeta del DNIE mediante el protocolo de autenticación interna-externa definido en CWA 14890-1. Este certificado estará ubicado en el directorio raíz de la tarjeta y no estará referenciado en la FAT; por lo tanto no estará accesible directamente por los interfaces estándar (PKCS11 o MS CSP).
- Certificados X509 de ciudadano (autenticación y firma) y claves privadas asociadas, que se generarán e insertarán durante el proceso de expedición del DNIE
- Datos de filiación, foto y firma manuscrita.

Nivel de Seguridad del chip.

- CC EAL 5+. El componente ha sido certificado por el esquema francés de evaluación y certificación de la T.I.

- CC EAL 4+ SOFT HIGH. La mascara se está certificando Common Criteria según el Perfil de Protección europeo para tarjetas inteligentes. Por el esquema de certificación Nacional.
- CWA 14169 – 3. SHCD. Dispositivo Seguro de Creación de Firma.
- CWA 14.890. Autenticación Mutua de Dispositivo.
- Sistema de Expedición. Acreditación por el Organismo Nacional de Certificación.

6. ¿quién lo expide y cuándo se obtiene?

La Dirección General de la Policía, además de todas las funciones que realiza relacionadas directa o indirectamente con la Seguridad del Estado y sus ciudadanos, en sus muy diversas vertientes, es también el organismo responsable en España de otras funciones de carácter administrativo, como lo es la expedición, control, renovación y gestión global del Documento Nacional de Identidad, así como otros documentos utilizados para la identificación de sus titulares, tanto en España como fuera del país.



6.1. ¿Quién expide el DNI electrónico?

La Comisaría General de Extranjería y Documentación, dependiente de la Dirección General de la Policía, es el departamento que se encarga de la expedición, control, renovación y gestión no sólo del DNI, sino también del

pasaporte y la tarjeta de residencia para los extranjeros que residan en España. Además, esta función la cumple este organismo en todo el territorio español, a través de sus oficinas de expedición, ya sean fijas o móviles.. La Dirección General de la Policía cuenta con 350 Oficinas de Expedición que se irán adaptando progresivamente al nuevo contexto.

6.2. ¿Cuándo estará operativo?

En marzo de 2006 se abre en Burgos la primera oficina piloto de implantación del nuevo documento.

El despliegue del DNI electrónico tendrá -esencialmente- un carácter geográfico y la previsión del Ministerio del Interior es que todas las Oficinas de Expedición estén emitiendo el DNI electrónico en la presente legislatura.

7. la formación, un eje básico de la cualificación profesional

La Dirección General de la Policía considera que su bien máspreciado es su equipo humano: su cualificación, su profesionalidad, su experiencia y el compromiso de su plantilla con la institución, lo que ésta representa y con el conjunto de la sociedad.

Para que todos sus miembros sigan siendo una referencia básica en sus capacidades profesionales, la Dirección General de la Policía tiene un programa de formación continuada y práctica durante todo el año, en muy diversas materias, como es el caso de las funciones administrativas de la Comisaría General de Extranjería y Documentación.

La implantación del nuevo DNI electrónico significará que a la formación programada para el período anual se le añada una específica sobre el nuevo modelo de documento que totalizará, inicialmente, más de 28.000 horas de formación para los miembros de la Dirección General de la Policía.

En este plan destaca el plan de adaptación técnica especial que está recibiendo la Oficina tecnológica, -que forman 50 personas, con una gran cualificación informática y formación específica en el campo técnico-, que lo sitúa en el deseado nivel de capacidad profesional.

En esta previsión inicial sobre el esfuerzo en formación acometido por la Dirección General de la Policía no se incluye la formación adicional –bastante más técnica- que recibirán los integrantes de la Oficina de Soporte técnico.

8. breves apuntes históricos

El Documento Nacional de Identidad es un servicio público, cuya gestión está legalmente encomendada en exclusiva al Cuerpo Nacional de Policía.

Desde su creación, hace más de 60 años, el DNI es gestionado por la Dirección General de Policía, encontrándose las Bases de Datos que soportan la gestión del DNI bajo su responsabilidad.

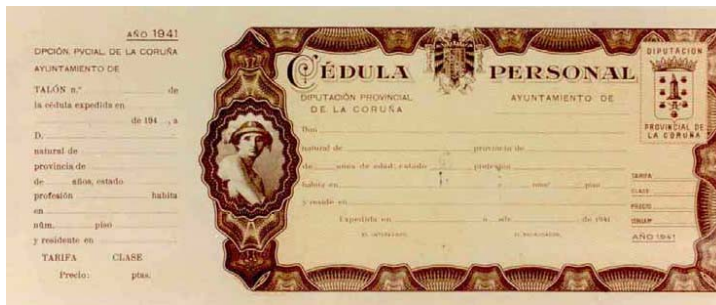
La Dirección General de la Policía cuenta con una extensa red para la expedición del DNI, superando las 300 oficinas en toda España.

El DNI acredita de forma inequívoca la identidad de su titular, es un elemento presente en la mayoría de las relaciones entre ciudadanos y de éstos con instituciones públicas y/o privadas.

El número de DNI es un dato que figura en el 97% de los registros de entidades y organizaciones, su uso está generalizado en todos los ámbitos del territorio español y es un referente obligado para la expedición de otros documentos como el pasaporte, el permiso de conducir, la seguridad social o la identificación fiscal (NIF).

Su obtención es obligatoria a partir de los 14 años, se renueva periódicamente: cada 5 años para los menores de 30 años; cada 10 años para los que tengan entre 30 y 60 años y a partir de los 70 años tienen validez permanente. Cada año se expiden del orden de 6 millones de documentos.

Las Cédulas Personales fueron el origen de los documentos de identidad en España, eran expedidas por la Diputaciones Provinciales y fueron el origen de los documentos de identidad en España.



A partir de 1944 el Documento Nacional de Identidad ha tenido sucesivas emisiones, en las cuales se han ido

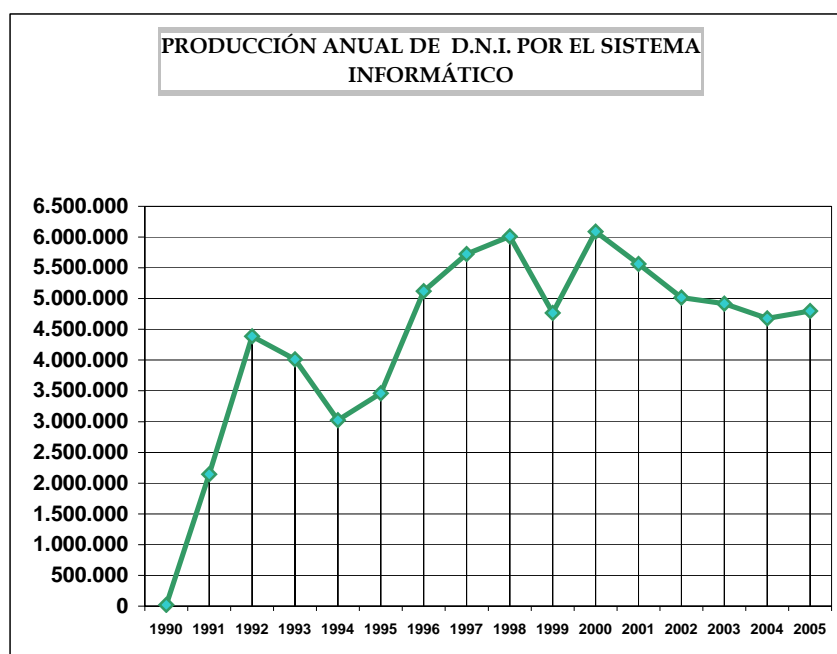
incorporando nuevas medidas para mejorar la seguridad. Por Real Decreto del 2 de marzo se crea el Documento Nacional de Identidad “con carácter nacional y eficiencia plena en la acreditación indubitada de la personalidad individual”.

La Unión Europea ha adoptado en los últimos años diversas iniciativas para el desarrollo e impulso de la Administración Electrónica. Con el mismo objetivo, el Gobierno Español ha puesto en marcha iniciativas donde la firma electrónica es una potente herramienta para impulsar el desarrollo de la sociedad de la información en España.



9. algunas cifras

- En España se han emitido un total de 51 millones de DNI, de los que continúan vigentes 31 millones.
- En 1990 comenzaron a expedirse los DNI por el sistema informático, introduciendo la imagen en color en los documentos en 1996.
- Para ello, la Dirección General de la Policía cuenta con 252 oficinas de expedición fijas y 96 móviles.
- Al año se emiten aproximadamente 6 millones de documentos.
- Para que esto sea posible hay unas 1.500 personas dedicadas a tareas relacionadas directa o indirectamente con la expedición del DNI, gran parte de ellas pertenecientes a los Cuerpos Generales de la Administración del Estado.



- En enero de 2005 se convocó el concurso público para el suministro de los componentes básicos del DNI electrónico, por un importe de 11.982.000 euros. La asistencia técnica para la coordinación y seguimiento de estos trabajos ha supuesto una inversión de 352.785,03 euros.
- La Dirección General de la Policía ha realizado trabajos de remodelación y adaptación de las Oficinas de Expedición del DNI y ha adquirido el equipamiento informático necesario para la elaboración de los nuevos documentos. Estas actuaciones han supuesto una inversión de 2.833.986,28 € y 1.089.747 € respectivamente.
- El conjunto de actuaciones previstas durante los próximos cuatro años que hasta la implantación total del DNI electrónico supondrá una inversión aproximada de 314 millones de euros. La partida principal, unos 219 millones de euros, corresponde al proyecto técnico.
- El nuevo DNI electrónico supone una inversión adicional de la Dirección General de la Policía de 60 millones de euros en nueva tecnología y equipamiento.
- Las nuevas tarjetas, soporte físico en el que irá el chip con los mismos datos de siempre, y el Servicio de Atención al Ciudadano, supondrán una inversión de 160 millones de euros.
- De aquí a 2008, se emitirán unos 9 nueve millones de nuevos DNI electrónicos.
- El coste unitario de cada nuevo DNI electrónico supera los 12 euros, además de otros costes fijos de la Dirección General de la Policía. Esto supone, aproximadamente, el doble que la tasa que el Estado cobra a los ciudadanos al renovarlo (6,60 euros).

10. el dni y la sociedad de la información en España

¿Qué es el DNI?

El Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita, desde hace más de 50 años, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular.

¿Ha sido siempre el mismo documento?

A lo largo de su vida, el Documento Nacional de Identidad ha ido evolucionado e incorporando las innovaciones tecnológicas disponibles en cada momento, con el fin de aumentar tanto la seguridad del documento como su ámbito de aplicación.

¿Cómo afectan las nuevas tecnologías al DNI?

Con la llegada de la Sociedad de la Información y la generalización del uso de Internet se hace necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que operamos cada día en el mundo físico.

Básicamente, ¿qué novedades incorpora el DNI electrónico?

1. Acredita electrónicamente y de forma indubitada la identidad de la persona

2. Permite firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita

A grandes rasgos, ¿qué diferencias hay entre el DNI tradicional y el electrónico?

Para responder a estas nuevas necesidades nace el Documento Nacional de Identidad electrónico (DNIe), similar al tradicional y cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de guardar de forma segura información y de procesarla internamente.

¿Cómo será el DNI electrónico que guardaremos en nuestras carteras?

Para poder incorporar este chip, el Documento Nacional de Identidad cambia su soporte tradicional (cartulina plastificada) por una tarjeta de material plástico, dotada de nuevas y mayores medidas de seguridad. A esta nueva versión del Documento Nacional de Identidad nos referimos como DNI, y electrónico nos permitirá, además de su uso tradicional, acceder a los nuevos servicios de la Sociedad de la Información, que ampliarán nuestras capacidades de actuar a distancia con las Administraciones Públicas, con las empresas y con otros ciudadanos.

¿Para que nuevas aplicaciones podremos utilizarlo?

En la medida que el DNI electrónico vaya sustituyendo al DNI tradicional y se implanten las nuevas aplicaciones, podremos utilizarlo para:

1. Realizar compras firmadas a través de Internet.
2. Hacer trámites completos con las Administraciones Públicas a cualquier hora y sin tener que desplazarse ni hacer colas.

3. Realizar transacciones seguras con entidades bancarias.
4. Acceder al edificio donde trabajamos.
5. Utilizar de forma segura nuestro ordenador personal.
6. Participar en un conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser.

¿Qué beneficio aporta el DNI electrónico al conjunto de los españoles?

El DNI electrónico es una oportunidad para acelerar la implantación de la Sociedad de la Información en España y situarnos entre los países más avanzados del mundo en la utilización de las tecnologías de la información y de las comunicaciones, lo que, sin duda, redundará en beneficio de todos los ciudadanos.

11. marco jurídico aplicable

Firma electrónica.

- Directiva 199/93/CE.
- Ley 59/2003.

Protección de Datos Personales y su procesamiento.

- Directivas 1995/46/CE, 97/66/EC, 2002/58/CE.
- Reglamento (EC) 45/2001.
- L.O.P.D. 15/1999 y Real Decreto 994/1999. Ley 32/2003 y 34/2002.

Específica del DNI.

- L.O. 1/1992, de Protección de la Seguridad Ciudadana.
- R.D. 1553/2005. Expedición del DNI y sus Certificados electrónicos,

GLOSARIO

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

Autenticación: procedimiento de comprobación de la identidad de un solicitante o titular de certificados de DNIE.

Certificado de Autenticación: Tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá a través de su certificado acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen, por tanto los terceros aceptantes y los prestadores de servicios no tendrán garantía del compromiso del titular del DNI con el contenido firmado. Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).

Este certificado puede ser utilizado también como medio de identificación para la realización de un registro que permita la expedición de certificados reconocidos por parte de entidades privadas, sin verse estas obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

Certificado electrónico: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Esta es la definición de la Ley 59/2003 que en este documento se extiende a los casos en que la vinculación de los datos de verificación de firma se hace a un componente informático.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Certificados de Identidad Pública: Emitidos como Certificados Reconocidos, vinculan una serie de datos personales del ciudadano a unas determinadas claves, para garantizar la autenticidad, integridad y no repudio. Esta información está firmada electrónicamente por la Autoridad de Certificación creada al efecto.

Ciudadano: toda persona física con nacionalidad española que solicita la expedición o renovación de un Documento Nacional de Identidad ante un funcionario de la Dirección General de la Policía.

Clave Pública y Clave Privada: la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

Clave de Sesión: clave que establece para cifrar una comunicación entre dos entidades. La clave se establece de forma específica para cada comunicación, sesión, terminando su utilidad una vez finalizada ésta.

Clave Personal de Acceso (PIN): Secuencia de caracteres que permiten el acceso a los certificados.

Datos de creación de Firma (Clave Privada): son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la Firma electrónica.

Datos de verificación de Firma (Clave Pública): son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma electrónica.

Directorio: Repositorio de información que sigue el estándar X.500 de ITU-T.

Dispositivo seguro de creación de Firma: instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Documento electrónico: conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información.

Documento de seguridad: documento exigido por la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal cuyo objetivo es establecer las medidas de seguridad implantadas, a los efectos de este documento, por la DGP como Prestador de Servicios de Certificación, para la protección de los datos de carácter personal contenidos en los Ficheros de la actividad de certificación que contienen datos personales (en adelante los Ficheros).

Encargado del Tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento de los ficheros.

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 personal.

Firma electrónica avanzada: es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

Firma electrónica reconocida: es aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Identificación: procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados de DNIe.

Identificador de usuario: conjunto de caracteres que se utilizan para la identificación unívoca de un usuario en un sistema.

Jerarquía de confianza: Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una AC de nivel superior garantiza la confiabilidad de una o varias de nivel inferior. En el caso de DNIe, la

jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.

Listas de Revocación de Certificados o Listas de Certificados Revocados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

Módulo Criptográfico Hardware de Seguridad: módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

Prestador de Servicios de Certificación: persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Punto de Actualización del DNIE: Terminal ubicado en las Oficinas de Expedición que permite al ciudadano de forma guiada, sin la intervención de un funcionario, la realización de ciertas operaciones con el DNIE (comprobación de datos almacenados en la tarjeta, renovación de los certificados de Identidad Pública, cambio de clave personal de acceso – PIN -, etc.).

Solicitante: persona que solicita un certificado para sí mismo.

Tercero Aceptante: persona o entidad diferente del titular que decide aceptar y confiar en un certificado emitido por DNIE.

Titular: ciudadano para el que se expide un certificado de identidad pública.