



COMISIÓN TÉCNICA
DE APOYO A LA
IMPLANTACIÓN
DEL DNI ELECTRÓNICO

GRUPO DE TRABAJO DE
COMUNICACIÓN Y DIVULGACIÓN

Versión 1.1
Fecha: 26 de junio de 2006

DNI electrónico

Guía de Referencia Básica



1. INTRODUCCIÓN

a. Concepto de identidad personal

Como declara el Art. 6 Declaración Universal de Derechos Humanos, “Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica”. Por tanto la identidad personal es un derecho de todo ciudadano y los Estados tienen la obligación de establecer los mecanismos adecuados para facilitársela.

Según la definición de la Real Academia Española de la Lengua, “La identidad es el conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás”, y también “Conciencia que una persona tiene de ser ella misma y distinta a las demás”.

Como se puede apreciar la identidad personal es un concepto importante que toma aún más valor en la actual Sociedad de la Información. De esta forma se entiende la necesidad de establecer los medios y mecanismos más adecuados para que el Estado otorgue esta identidad personal a sus ciudadanos.

Otorgar identidad personal a los ciudadanos adquiere una nueva dimensión cuando se trata de establecerla para un uso no presencial en medios telemáticos. Y aunque la identidad siempre es física, es necesario establecer mecanismos y procedimientos electrónicos para verificarla en estos nuevos ámbitos.

El nacimiento del Documento Nacional de Identidad electrónico (DNIe) viene a cubrir la necesidad de otorgar identidad personal a los ciudadanos para su uso en la nueva Sociedad de la Información, además de servir de dinamizador de la misma.

b. Aceptación social del DNI



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 en un altísimo porcentaje 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.

c. Antecedentes: DNI tradicional versus DNI electrónico

Como establece el artículo 1 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”*.

De la lectura de este artículo se comprueba que esta característica del DNI tradicional, se mantiene en toda su extensión en el DNI electrónico, incrementada en las nuevas funciones de firma electrónica de documentos, en los términos previstos en la [Ley 59/2003, de 19 de diciembre, de firma electrónica](#).

d. Concepto y funciones básicas

[La Ley 59/2003, de 19 de diciembre, de firma electrónica](#), ha venido a atribuir al Documento Nacional de Identidad nuevos efectos y utilidades:

- Crear un documento que certifique la identidad del ciudadano no sólo en el mundo físico, sino también ante transacciones telemáticas, permitiendo firmar todo tipo de documentos electrónicos. Usando un dispositivo seguro de creación de firma, la firma electrónica que se efectúe mediante el DNI electrónico tendrá efectos equivalentes a los de una firma manuscrita.
- Expedir el DNI electrónico en un solo acto administrativo, reduciendo así el tiempo empleado para su obtención.
- Interoperabilidad con los proyectos europeos de identificación digital.
- Fomentar la confianza en las transacciones electrónicas.



- Aceptación por parte de todas las Administraciones Públicas y Entidades de Derecho Público vinculadas o dependientes de las mismas del uso del DNI electrónico. (E.j. para hacer la declaración de la renta, pedir un certificado de empadronamiento, dar de alta en el registro de nacimientos o reclamar el derecho a la pensión).

e. La firma electrónica: novedad. Conceptos básicos

La Firma electrónica es un sistema de acreditación que permite verificar la identidad de las personas con el mismo valor que la firma manuscrita, autenticando las comunicaciones generadas por el firmante.

Por otra parte 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.

Asimismo la Ley distingue entre “firma electrónica avanzada” y “firma electrónica reconocida”:

- (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.
(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 consignados en papel.

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 (clave privada) y pone a disposición del público la otra (clave pública).



- El emisor obtiene un resumen del mensaje a firmar con una función llamada “hash” (resumen). El resumen es una operación que se realiza sobre un conjunto de datos, 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”.
- El emisor cifra el resumen del mensaje con la clave privada. Ésta es la firma electrónica que se añade al mensaje original.
- El receptor, al recibir el mensaje, obtiene de nuevo su resumen mediante la función “hash”. Además descifra la firma utilizando la clave pública del emisor obteniendo el resumen que el emisor calculó. 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.

f. ¿Qué tiene y que no tiene el DNI electrónico?

El DNI electrónico contiene la siguiente información:

- Certificados X509v3 de ciudadano (autenticación y firma) y claves privadas asociadas, que se generarán e insertarán durante el proceso de expedición del DNLe:
 - Certificado de autenticación
El Ciudadano podrá, a través de su Certificado de Autenticación, 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.
 - Certificado de firma electrónica reconocida
Permitirá realizar y firmar acciones y asumir compromisos de forma electrónica, pudiéndose comprobar la integridad de los documentos firmados por el ciudadano haciendo uso de los instrumentos de firma incluidos en él.

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

- En el cuerpo central de la tarjeta:
 - Primer apellido
 - Segundo apellido
 - Nombre
 - Sexo



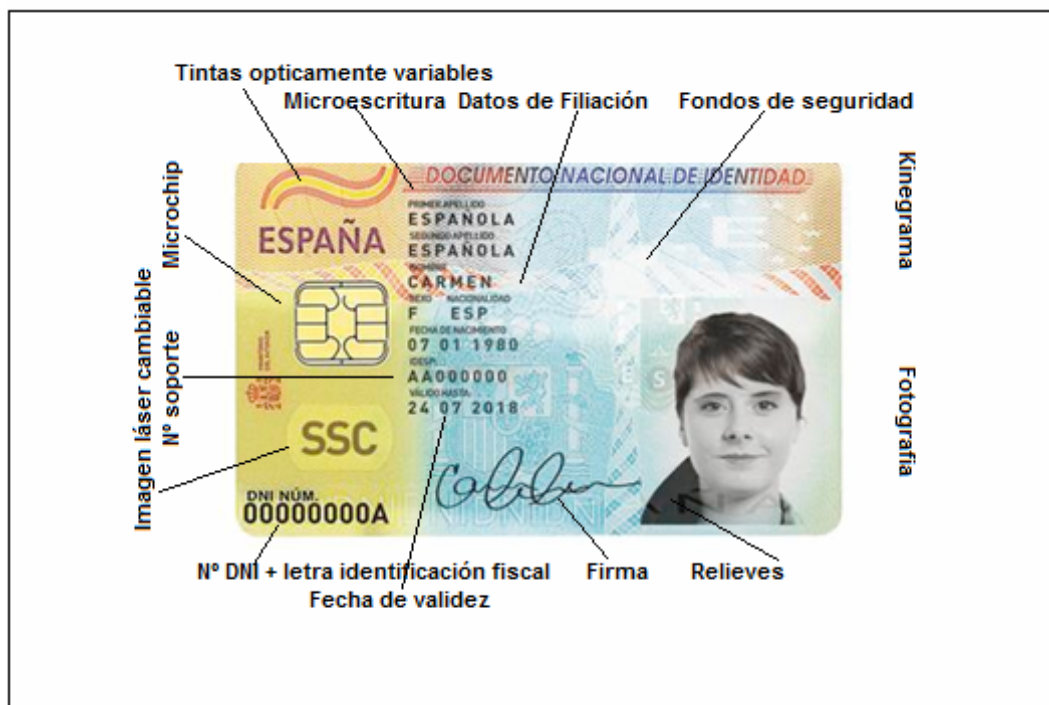
- Nacionalidad
- Fecha de nacimiento
- Número de serie del soporte físico de la tarjeta (IDESP)
- Fecha de validez del documento

En la esquina inferior izquierda:

- Número del Documento Nacional de Identidad del Ciudadano

En el espacio destinado a la impresión de imagen láser cambiante (CLI) situada debajo del chip:

- 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)



El reverso de la tarjeta contiene los siguientes elementos:



- En la parte superior:
 - Lugar de nacimiento
 - Provincia–País
 - Nombre de los padres
 - Domicilio
 - Lugar de domicilio
 - Provincia–país del domicilio
 - Código del equipo de expedición del DNle
- Información impresa OCR–B para lectura mecanizada sobre la identidad del ciudadano según normativa OACI para documentos de viaje.

El DNI electrónico no contiene ninguna otra información relativa a datos personales ni de cualquier otro tipo (sanitarios, fiscales, tráfico, etc.)



2. Descripción funcional del DNI electrónico

a. Nuevas capacidades. Identificación.

El DNI electrónico, además de la capacidad de identificación física de su titular, posee la capacidad de identificación en medios telemáticos y de firmar electrónicamente como si de una firma manuscrita se tratase. De esta forma garantiza que la personalidad del firmante no es suplantada.

Asimismo la firma electrónica permite proteger la información enviada a través de un medio telemático.



b. Firma electrónica.

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.

La firma electrónica permite que tanto el receptor como el emisor de un contenido puedan identificarse mutuamente con la certeza de que son ellos los que están interactuando, evita que terceras personas intercepten esos contenidos y que los mismos puedan ser alterados, así como que alguna de las partes pueda "repudiar" la información que recibió de la otra y que inicialmente fue aceptada.

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.

A su vez, se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

c. Certificados electrónicos. Una breve descripción.

Son los documentos expedidos por los prestadores de servicios de certificación que relacionan las herramientas de firma electrónica que tiene cada usuario con su identidad, dándole a conocer como firmante en el ámbito telemático

d. Vida útil

Al hablar de vida útil se deben contemplar dos aspectos.

En primer lugar, la validez del DNI electrónico no varía según el DNI actual, manteniéndose los mismos periodos que actualmente (Artículo 6. Validez, RD 1553/2005, de 23 de diciembre), es decir:

- a) Cinco años, cuando el titular no haya cumplido los treinta al momento de la expedición o renovación
- b) Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.
- c) Permanente cuando el titular haya cumplido los setenta años.



De forma excepcional se podrá otorgar validez permanente a los mayores de 30 años que acrediten la condición de gran inválido, o de un año en determinadas circunstancias.

En segundo lugar está la validez de los certificados contenidos en el chip de la tarjeta del DNI electrónico que tendrán un período de vigencia de treinta meses. (Artículo 12. *Validez de los certificados electrónicos*, RD 1553/2005, de 23 de diciembre)

e. Marco legal básico

El marco legal básico del DNI electrónico es el siguiente:

- **Directiva 1999/93/CE del Parlamento Europeo y del Consejo**, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica.
- **Ley 59/2003**, de 19 de diciembre, de Firma Electrónica.
- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de los Datos.
- **Real Decreto 1553/2005**, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica.
- **Real Decreto 1586/2009**, de 16 de octubre, por el que se modifica el Real Decreto 1553/2005.

3. ¿Qué ventajas nos ofrece el DNI electrónico?

- En las relaciones entre ciudadanos
 - La firma electrónica del DNI electrónico permite garantizar la identidad de la persona que realiza una gestión, así como la integridad del contenido de los mensajes que envía. Por tanto los ciudadanos podrán consultar datos de carácter personal, realizar trámites u otras gestiones o acceder a diferentes servicios públicos y privados.
 - Proporciona el máximo grado de confidencialidad y seguridad en Internet.
 - Identifica a las partes que se conectan telemáticamente.
 - Da acceso a una inmejorable oferta de servicios en el ámbito de la gestión de los derechos de autor.
- En las relaciones con las Administraciones Públicas.



- El Art. 16.2 de la Ley 59/2003 de Firma Electrónica indica que:” La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados”
- La Administración General del Estado será uno de los principales proveedores de servicios que se podrán utilizar con el DNI electrónico, de esta forma su utilización supone una ventaja en los trámites con la Administración Pública, en la que ya no sería necesario la presencia física para garantizar la identidad.
- En las relaciones con las empresas
 - Las empresas deberán desarrollar diferentes servicios basados en la identificación y firma electrónica, de forma que dinamicen la relación comercial con sus clientes. Estos servicios podrán ser ofrecidos con la máxima seguridad.
 - Desde el punto de vista empresarial y comercial el DNI electrónico se convierte en una herramienta fundamental en las relaciones en el sector privado.

4. Descripción física

El propósito de la tarjeta soporte del DNIE es contener 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.
 - La tarjeta física del DNI electrónico sigue el estándar ISO-7816-1
 - Está fabricada en policarbonato, que es un material que permite su uso continuado y frecuente sin sufrir deterioro, durante el tiempo de vigencia del DNI, es decir, 10 años.
 - La personalización de la tarjeta se realiza mediante la grabación en el cuerpo de la tarjeta con láser de los datos de filiación, fotografía y firma manuscrita. Este sistema de personalización garantiza la imposibilidad de manipulación de estos datos.



- Cuenta con las más modernas medidas de seguridad ante la manipulación y falsificación del documento, muchas de ellas fácilmente identificables por cualquier persona sin ningún procedimiento especial. El conjunto de todas las medidas hace del DNI electrónico un documento altamente seguro, tanto desde el punto de vista físico, como electrónico.
2. El chip del DNI electrónico, cuyas características son
- Chip ST19WL34
 - Sistema operativo DNle v1.1
 - Capacidad de 32K.
 - Contenido del chip:

La información en el chip está distribuida en tres zonas con diferentes niveles y condiciones de acceso:

- Zona pública: Accesible en lectura sin restricciones, contenido:
 - Certificado CA intermedia emisora.
 - Claves Diffie–Hellman.
 - Certificado x509 de componente
 - Zona privada: Accesible en lectura por el ciudadano, mediante la utilización de la Clave Personal de Acceso o PIN, contenido:
 - Certificado de Firma (No Repudio).
 - Certificado de Autenticación (Digital Signature).
 - Zona de seguridad: Accesible en lectura por el ciudadano, en los Puntos de Actualización del DNle.
 - Datos de filiación del ciudadano (los mismos que están impresos en el soporte físico del DNI), contenidos en el soporte físico del DNI.
 - Imagen de la fotografía.
 - Imagen de la firma manuscrita.
 -
- **DATOS CRIPTOGRÁFICOS:** Claves de ciudadano
 - Clave RSA pública de autenticación (Digital Signature).
 - Clave RSA pública de no repudio(ContentCommitment).



Clave RSA privada de autenticación (Digital Signature).

Clave RSA privada de firma (ContentCommitment).

Patrón de impresión dactilar.

Clave Pública de root CA para certificados card-verificables.

Claves Diffie-Hellman.

- **DATOS de GESTIÓN:**

Traza de fabricación.

Número de serie del soporte.

El chip de la tarjeta almacena los siguientes certificados electrónicos:

- **Certificado de Componente.** Su propósito es la autenticación de la tarjeta del DNI electrónico mediante el protocolo de autenticación mutua definido en CWA 14890.
 - Permite el establecimiento de un canal cifrado y autenticado entre la tarjeta y los Drivers.
 - Este certificado no estará accesible directamente por los interfaces estándar (PKCS11 o CSP).
- **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 de firma.** Este certificado es el que utilizaremos para la firma de documentos garantizando la integridad del Documento y el No repudio de origen.

Es un certificado X509v3 estándar, que tiene activo en el Key Usage el bit de ContentCommitment (No Repudio) y que esta asociado a un par de claves pública y privada, generadas en el interior del CHIP del DNI.

Es este Certificado expedido como certificado reconocido y creado en un Dispositivo Seguro de Creación de Firma, el que convierte la firma electrónica avanzada en firma electrónica reconocida, permitiendo su equiparación legal con la Firma Manuscrita (Ley 59/2003 y Directiva 1999/93/CE).

5. Proceso de expedición

Proceso de expedición

- Dónde y cómo se expide. Proceso en un solo paso
 - El DNI electrónico se expide en los centros en los que actualmente se está realizando (equipos de expedición y equipos móviles)
 - El DNI electrónico se expide en un solo acto administrativo, es decir en una sola visita al centro de expedición.
- Qué hace falta llevar.

Para solicitar la primera expedición del Documento Nacional de Identidad será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de los siguientes documentos:

- Certificación literal de nacimiento expedida por el Registro Civil correspondiente o, en su caso, Certificado de inscripción de la nacionalidad española. A estos efectos únicamente serán admitidas las certificaciones expedidas con una antelación máxima de seis meses a la fecha de



presentación de la solicitud de expedición del Documento Nacional de Identidad y que contengan la anotación de que se ha emitido a los solos efectos de la obtención de este documento.

- Una fotografía reciente, en color, del rostro del solicitante, tamaño 32 por 26 milímetros con fondo uniforme, blanco y liso, tomadas de frente con la cabeza totalmente descubierta y sin gafas de cristales oscuros o cualquier otra prenda que pueda impedir o dificultar la identificación de la persona.
- Certificado o volante de empadronamiento del Ayuntamiento donde el solicitante tenga su domicilio, expedido con una antelación máxima de tres meses a la fecha de la solicitud del Documento Nacional de Identidad.
- Los españoles residentes en el extranjero acreditarán el domicilio mediante la presentación de un certificado de acreditación de residencia que a estos efectos se expiden por la Representación Diplomática o Consular donde se hallen inscritos como residentes.

La renovación se llevará a cabo mediante la presencia física del titular del Documento, que deberá abonar la tasa correspondiente y aportar los siguientes documentos:

- Una fotografía reciente, en color, del rostro del solicitante, tamaño 32 por 26 milímetros con fondo uniforme, blanco y liso, tomadas de frente con la cabeza totalmente descubierta y sin gafas de cristales oscuros o cualquier otra prenda que pueda impedir o dificultar la identificación de la persona.
- El DNI anterior.
- En caso de cambio de domicilio, respecto del que figure en el Documento anterior, certificado o volante de empadronamiento del Ayuntamiento donde el solicitante tenga su domicilio (la validez de este documento es de 3 meses a partir de la fecha de su expedición). La presentación de este documento no será necesaria si el interesado autoriza, en el momento de la tramitación del DNI, a que por el equipo de expedición se acceda al Sistema de Verificación de Datos de Residencia, a efectos de consultar los datos de su domicilio.
- En caso de variación de datos de filiación, partida literal de nacimiento del Registro Civil, expedido con una antelación máxima de seis meses a la fecha de solicitud del DNI.
- El extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido en la forma y con los requisitos indicados para la renovación. En estos casos, el nuevo DNI tendrá la misma validez que



el documento al que sustituye, salvo que éste se hallase en los últimos 90 días de su vigencia y si el DNI extraviado o sustraído era del modelo anterior se ha de aportar una fotografía más y confeccionar un impreso que se entrega en la propia oficina de expedición.

-
- Los españoles residentes en el extranjero, además de los documentos indicados, deberán aportar el certificado de acreditación de residencia a que se hace referencia para la primera inscripción.

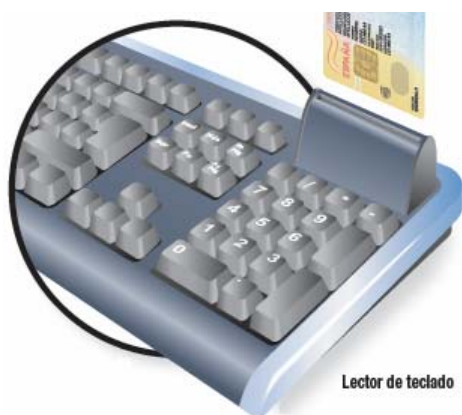
6. Tipos de dispositivos, sistemas operativos y estándares.

Para la utilización del DNI electrónico es necesario contar con determinados elementos hardware y software que nos van a permitir el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

a) Elementos hardware

El DNI electrónico requiere el siguiente equipamiento físico:

- Un Ordenador personal (Intel –a partir de Pentium III– o tecnología similar).
- Un lector de tarjetas inteligentes que cumpla el estándar ISO-7816. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados vía USB) o bien a través de una interfaz PCMCIA.



Lector de teclado



Lector USB

Para elegir un lector que sean compatible con el DNI electrónico, verifique que, al menos:



- Cumpla el estándar ISO 7816 (1, 2 y 3)
- Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1)
- Soporta velocidades de comunicación mínimas de 9.600 bps.
- Soporta los estándares:
 - API PC/SC (Personal Computer/Smart Card)
 - CSP (Cryptographic Service Provider, Microsoft)
 - API PKCS#11

b) Elementos software

- Sistemas operativos

El DNI electrónico puede operar en diversos entornos:

- Microsoft Windows (Windows XP, Windows 2000)
- Linux
- Unix
- Mac

- Navegadores

El DNI electrónico es compatible con todos los navegadores:

- Microsoft Internet Explorer (versión 6.0 o superior)
- Mozilla Firefox (versión 1.5)
- Netscape (versión 4.78 o superior)

- Controladores / Módulos criptográficos

Para poder interactuar adecuadamente con las tarjetas criptográficas en general y con el DNI electrónico en particular, el equipo ha de tener instalados unas "piezas" de software denominadas módulos criptográficos.

- En un entorno Microsoft Windows, el equipo debe tener instalado un servicio que se denomina "Cryptographic Service Provider" (CSP).
- En los entornos UNIX / Linux o MAC podemos utilizar el DNI electrónico a través de un módulo criptográfico denominado PKCS#11



Tanto el CSP como el PKS#11 específico para el DNI electrónico podrán obtenerse en la dirección www.dnielectronico.es/descargas/

Adicionalmente, para operar con un lector de tarjetas inteligentes, será necesario instalar un driver que, normalmente, se distribuye con el propio lector.

7. Uso del DNI electrónico

Uso del DNI electrónico

Tal y como recoge la Declaración de Prácticas de Certificación del DNI electrónico, los certificados electrónicos podrán utilizarse:

- **Como medio de Autenticación de la Identidad.**

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.

- **Como medio de firma electrónica de documentos.**

Mediante la utilización del Certificado de Firma (nonRepudition), el receptor de un mensaje firmado electrónicamente puede verificar la autenticidad de esa firma, pudiendo de esta forma demostrar la identidad del firmante sin que éste pueda repudiarlo.

- **Como medio de certificación de Integridad de un documento.**

Permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. La garantía de la integridad del documento se lleva a cabo mediante la utilización de funciones resumen (hash), utilizadas en combinación con la firma electrónica. Este esquema permite comprobar si un mensaje firmado ha sido alterado posteriormente a su envío.

Para tal fin, utilizando la clave privada del ciudadano, se firma un resumen del documento, de forma tal que cualquier alteración posterior del documento dará lugar a una alteración del resumen.

El Certificado de Identidad Pública español (DNI electrónico) contribuirá, necesariamente a la existencia de empresas prestadoras de servicios de valor añadido ya que el DNI electrónico no facilitará en ningún caso los denominados "sobres" (sistemas de cifrado, sellos de tiempo, etc.)



De la misma forma favorecerá la aparición de iniciativas privadas que presten servicios de certificación a los ciudadanos. Esto se conseguirá en base a reconocer al DNI electrónico como medio suficiente para acreditar, la identidad y los demás datos personales de los interesados, pudiendo ser utilizado como medio de identificación para la realización de un registro fuerte 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.

Escenario

Imaginemos la siguiente situación: un ciudadano establece una comunicación a través de Internet con un organismo de la Administración Pública (o una Entidad Privada) que ofrece un servicio telemático para que el ciudadano cumplimente un trámite administrativo que requiere su consentimiento explícito para la realización.

Este escenario plantea el uso de los dos tipos de certificados electrónicos por parte del ciudadano:

- Certificado de Autenticación (Digital Signature), cuyo propósito exclusivo es el de identificar al ciudadano. Este certificado no vincula al ciudadano en ninguna forma y es exclusivamente utilizado para el establecimiento de canales privados y confidenciales con los prestadores de servicio. Permite cerrar el túnel SSL con el certificado del ciudadano y el del prestador de servicios, así como facilitar su identidad a éste último.
- Certificado de Firma (nonRepudiation), cuyo fin es permitir al ciudadano firmar trámites o documentos. Este certificado (certificado cualificado según ETSI y las RFC3039, RFC3739) permite sustituir la firma manuscrita por la electrónica en las relaciones del ciudadano con terceros (Ley 59/2003, de firma electrónica, artículos 3.4 y 15.2).

Descripción de Uso

Asumiendo que:

- El ciudadano dispone de un DNI con capacidades electrónicas (criptográficas)
- Está conectado al servicio telemático de forma remota a través de Internet
- Dispone de una instalación local con un lector de tarjetas inteligentes compatible (PC/SC)
- Cuenta con el CSP o el PKCS#11 del DNI electrónico.



a) Establecimiento de conexión privada con Organismo Público o Entidad Privada.

El siguiente esquema de comunicaciones establece el protocolo a seguir para el establecimiento de un canal privado y autenticado entre el ciudadano y el Organismo Público o Entidad Privada. El canal establecido queda autenticado en ambos extremos por el uso de certificados que garantizan la identidad de las partes:

1. El Ciudadano hace una petición de conexión segura autenticada
2. El Organismo Público (o Entidad Privada) crea un mensaje autenticado y lo envía al ciudadano
3. El Ciudadano verifica la validez del certificado de servidor ofrecido
4. Se genera la clave de sesión y cifrado de la misma con la clave pública del Organismo Público (o Entidad Privada).
5. Se construye el mensaje de intercambio de claves.
6. El Ciudadano introduce el DNI electrónico en el lector y, con el certificado electrónico de autenticación, valida el mensaje de intercambio de claves.
7. Se establece el canal privado.
8. El Organismo Público (o Entidad Privada) verifica el mensaje de establecimiento de sesión.
9. El Organismo Público (o Entidad Privada) comprueba en la Autoridad de Validación el estado validez del Certificado de Autenticación del Ciudadano.
10. Se establece un canal seguro, se cierra el túnel SSL.

Tal y como queda reflejado en el esquema anterior, el proceso de autenticación entre ambas partes para el establecimiento de un canal seguro requiere del uso de:

- Certificado de Organismo Público (o Entidad Privada): Este certificado asociado al servidor del Organismo o Entidad garantiza que el ciudadano se esta conectando a dicho organismo y no a otro. El certificado utilizado por el Organismo o Entidad no es en ningún caso emitido por la DGP o el Ministerio del Interior, la veracidad de este certificado deberá ser garantizada por una Autoridad de Certificación diferente de la DGP y sujeta a la Ley de Firma Electrónica 59/2003 en el marco de obligaciones aplicables a los prestadores de servicios de certificación.



- Certificado de autenticación del ciudadano. El ciudadano para autenticarse frente al Organismo (o Entidad Privada) dispone de un certificado con capacidad de autenticación. De esta forma el Organismo (o Entidad Privada) podrá determinar la identidad del ciudadano para ofrecerle un servicio personalizado. La veracidad de este certificado vendrá determinada por la Dirección General de la Policía.

Las partes implicadas para el establecimiento del canal privado son:

- **DNI electrónico:** Dispositivo de firma y autenticación segura en posesión del ciudadano emitido por la Institución del DNI, que contendrá:
 - Conjunto de claves privadas al ciudadano.
 - Conjunto de certificados del ciudadano.
 - Elementos de seguridad para garantizar la integridad del documento frente a posibles alteraciones.
- **Ciudadano:** Persona física titular del DNI electrónico.
- **Organismo Público** (o Entidad Privada): Proveedor de servicios.
- **Autoridad de Validación:** Servicio informativo del estado de validez de los certificados del ciudadano.

Usabilidad

El protocolo descrito en el esquema corresponde al establecimiento de una sesión SSL (Secure Socket Layer). La elección de este mecanismo viene determinada por que prácticamente el 100% de los servidores y clientes utilizados disponen de esta capacidad.

Este protocolo permite el establecimiento de canales privados con los proveedores de servicios, organismos públicos u otros. Si bien, existen dos tipos de canales:

1. **Autenticación Servidor:** En esta modalidad, sólo el servidor requiere tener un certificado por lo que la identidad del cliente, el ciudadano en nuestro caso, será anónima.

2. **Autenticación Servidor–Cliente:** Requiere que tanto el proveedor de servicios se autentique frente al cliente (ciudadano), como que el cliente se autentique frente al servidor. **(Este es el ideal recomendado)**



La diferencia real en cuanto a usabilidad estriba principalmente en que si el proveedor de servicios, puede determinar con garantía la identidad del ciudadano estará en disposición de ofrecerle información personalizada.

La utilización del certificado de Autenticación del DNI electrónico garantiza la identidad del ciudadano, y podrá ser utilizado por los proveedores de servicios para establecer reglas de acceso a la información en base a la identidad del mismo.

b) Firma de Trámites Administrativos con DNI electrónico.

El siguiente esquema establece el protocolo a seguir para la firma de formularios electrónicos, mediante el uso del DNI electrónico, cumpliendo con la normativa sujeta al uso de certificados cualificados:

1. El Organismo Público (o Entidad Privada) envía el formulario para el trámite administrativo
2. El Ciudadano cumplimenta el formulario y lo envía
3. El Organismo Público (o Entidad Privada) reconstruye el formulario en formato texto y lo reenvía nuevamente al ciudadano
4. El Ciudadano verifica que el trámite administrativo se corresponde exactamente con el cumplimentado
5. Se solicita al ciudadano la firma electrónica del formulario
6. El Ciudadano introduce su clave de acceso personal (PIN) para el acceso al certificado de Firma (nonRepudiation).
7. El DNI electrónico firma electrónicamente el formulario.
8. El Ciudadano envía formulario firmado al Organismo Público (o Entidad Privada)
9. El Organismo Público (o Entidad Privada) verifica validez de la firma, para comprobar la integridad del formulario
10. El Organismo Público (o Entidad Privada) comprueba en la Autoridad de Validación el estado de validez del certificado de Firma (nonRepudiation) del ciudadano
11. Si es correcto, continuar el procedimiento...

Conviene recordar que para llevar a cabo un proceso de firma electrónica debemos disponer de una aplicación informática que nos permita realizar esta funcionalidad.



Hay dos alternativas tecnológicas para disponer de la funcionalidad de firma electrónica:

- La funcionalidad de firma electrónica se logra a través de una aplicación informática previamente instalada en nuestro equipo.
- La funcionalidad de firma electrónica está incluida en el proceso general del prestador de servicios telemáticos, por lo que no es necesario descargar e instalar ninguna aplicación de firma electrónica.

Confirmación por parte del organismo de la correcta recepción del trámite.

El trámite administrativo se completa con la entrega por parte del Organismo receptor del formulario firmado con acuse de recibo. Aunque este trámite es ajeno al DNI electrónico, parece necesario que el prestador del servicio ofrezca garantía al ciudadano de la correcta realización del trámite efectuado. Dentro de unas buenas prácticas el prestador de servicios deberá proporcionar al ciudadano un recibo indicando que su trámite ha sido aceptado.

El siguiente esquema muestra el protocolo a seguir entre las diferentes partes:

1. El Organismo Público (o Entidad Privada) confecciona el recibo para el trámite cumplimentado por el ciudadano
2. El Organismo Público (o Entidad Privada) firma el recibo
3. El recibo es firmado y sellado por una Tercera parte de confianza, denominada Autoridad de Sellos de Tiempo (que garantiza el instante exacto en el que un trámite fue aceptado por el prestador de servicios, y debe ser evidentemente una entidad externa a dicho prestador y reconocida en el ámbito de la legislación española)
4. Se envía al Ciudadano el recibo firmado y sellado

8. Verificación

La Autoridad de Validación es el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación.

La información sobre los certificados electrónicos revocados (no vigentes) se almacena en las denominadas listas de revocación de certificados (CRL).

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.

Así, la Autoridad de Certificación (Ministerio del Interior – Dirección General de la Policía) no tiene en modo alguno acceso a los datos de las transacciones que se realicen con los certificados que ella emite y las Autoridades de Validación no tiene acceso a la identidad de los titulares de los certificados electrónicos que maneja, reforzando –aún más si cabe– la transparencia del sistema.

Para la validación del DNI electrónico se dispone de dos prestadores de Servicios de Validación:

- Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, que prestará sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas.
- Ministerio de Administraciones Públicas, que prestará los servicios de validación al conjunto de las Administraciones Públicas.

Adicionalmente, la Entidad Pública Empresarial Red.es podría completar los servicios de validación en un futuro próximo.

La prestación de estos servicios de validación se realiza en base a Online Certificate Status Protocol (OCSP), lo que, en esencia, supone que un cliente OCSP envía una petición sobre el estado del certificado a la Autoridad de Validación, la cual, tras consultar su base de datos, ofrece – vía http – una respuesta sobre el estado del certificado.

El servicio de validación está disponible de forma ininterrumpida todos los días del año.

9. Seguridad

– Funciones de seguridad accesibles

Para hacer uso del DNI electrónico en los términos expuestos anteriormente, éste provee las siguientes funciones de seguridad:

1. Autenticación

La tarjeta DNLe dispone de distintos métodos de autenticación, mediante los que una entidad externa demuestra su identidad, o el conocimiento de algún dato secreto almacenado en la tarjeta. La correcta realización de cada uno de estos métodos, permite obtener unas



condiciones de seguridad, que podrán ser requeridas para el acceso a los distintos recursos de la tarjeta.

- Autenticación de usuario (PIN)

La tarjeta DNle soporta verificación de usuario (CHV- Card Holder verification). Esta operación es realizada comprobando el código facilitado por la entidad externa a través del correspondiente comando.

Cada código CHV tiene su propio contador de intentos. Tras una presentación válida de PIN, el contador de reintentos correspondiente es automáticamente puesto a su valor inicial (típicamente = 3). El contador de intentos es decrementado cada vez que se realiza una presentación errónea, pudiendo llegar a bloquearlo si el contador llega a cero. Es posible desbloquear un código tras una correcta presentación de la huella dactilar del usuario, que en este caso actúa de código de desbloqueo. A su vez estas presentaciones de huellas tienen su propio contador de intentos. Si el número de intentos de presentación de huella dactilar se agota, no será posible realizar la operación de desbloqueo. Es posible cambiar el código de CHV a un nuevo valor presentando el valor actual o presentando la huella dactilar.

El código PIN es personal e intransferible, por tanto, únicamente debe ser conocido por el titular de la tarjeta en cuestión.

- Autenticación de usuarios mediante datos biométricos

La tarjeta DNle permite realizar una identificación biométrica del titular de ésta, si bien esta función sólo estará disponible en puntos de acceso controlados.

La aplicación que accede al DNle, una vez conocida la información sobre las huellas contenidas en la tarjeta, decide sobre que huella va a proceder a verificar, solicitando al portador que coloque el dedo adecuado. Tras obtener los datos biométricos desde el dispositivo lector de huellas, presenta la información biométrica a la tarjeta a través del correspondiente comando. Tras las comprobaciones iniciales de condiciones de uso y seguridad, la tarjeta procede, mediante su algoritmo Match on Card, a evaluar la correspondencia entre la huella presentada y la referencia.

Si la evaluación supera el umbral, la verificación es correcta. En caso contrario, la tarjeta anota una presentación errónea sobre esa huella devolviendo el número de intentos restantes.

- Autenticación de aplicación



El propósito de este método de autenticación es que la entidad externa demuestre tener conocimiento del nombre y valor de un código secreto. Para realizar esta autenticación de aplicación, se utiliza un protocolo de desafío–respuesta, con los siguientes pasos:

- La aplicación pide un desafío a la tarjeta
 - La aplicación debe aplicar 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
- Autenticación mutua

Este procedimiento permite que cada una de las partes (tarjeta y aplicación externa) confíe en la otra, mediante la presentación mutua de certificados, y su verificación.

En el proceso, 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, que podrán seleccionarse implícitamente en función de la secuencia de comandos, o explícitamente, indicando su identificador de algoritmo en un comando de gestión de entorno de seguridad anterior (MSE).

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’, 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)

2. Securización de mensajes

La tarjeta DNle permite la posibilidad de establecer un canal seguro entre el terminal y la tarjeta que securice los mensajes transmitidos. Para el establecimiento es necesaria la autenticación previa del terminal y la tarjeta, mediante el uso de certificados. Durante la presencia del canal seguro los mensajes se cifran y autentican, de tal forma que se asegura una comunicación “una a uno” entre los dos puntos originarios del canal.

El canal seguro puede ser requerido por la aplicación o puede ser una restricción de acceso impuesta a algún recurso de la tarjeta



Para el establecimiento del canal seguro, en primer lugar, se realiza un intercambio de las claves públicas de la tarjeta y el terminal mediante certificados que serán verificados por ambas partes. A continuación se realiza un protocolo de autenticación mutua, con intercambio de semillas para la derivación de una semilla común que dé lugar a las claves de sesión de cifrado y autenticado

Una vez concluido el protocolo para el establecimiento de la semilla común todos los mensajes deben transmitirse securizados.

3. Desbloqueo y cambio de PIN

Se permite el cambio de PIN, mediante la presentación del valor antiguo. Es posible también el cambio de PIN bajo determinadas condiciones tras la realización de una verificación biométrica.

Debido a la criticidad de esta operación, el cambio de PIN se ha de realizar siempre en condiciones de máxima confidencialidad y en terminales específicamente habilitados a tal efecto o con las debidas condiciones de seguridad, exigiéndose por tanto, el establecimiento de un canal seguro.

El cambio de PIN, haciendo uso de la huella dactilar (desbloqueo), únicamente está permitido en dispositivos autorizados por la Dirección General de la Policía (DGP) y no se puede realizar, bajo ningún concepto, en otros terminales.

4. Funcionalidad criptográfica

- Claves RSA

La tarjeta DNle es capaz de generar y gestionar claves RSA. La generación de la pareja de claves RSA sigue el estándar PKCS#1 v1.5. Se usa el algoritmo Miller-Rabin como test de primalidad.

- Hash

La tarjeta DNle es capaz de realizar hash de datos con el algoritmo SHA1. Es posible realizar todo el proceso en la tarjeta o finalizar un hash calculado externamente. Después de finalizar cualquier operación de hash, el código resultante es almacenado en la memoria de la tarjeta para ser usado posteriormente por un comando. El hash sólo permanece en memoria hasta la siguiente operación.

- Firmas electrónicas



La tarjeta DNle tiene capacidad para la realización de firmas electrónicas de dos modos diferentes:

- Modo raw
- Modo relleno PKCS#1

5. Intercambio de claves

La operación de intercambio de claves es usada para compartir claves simétricas o de sesión entre dos entidades. Es posible cifrar una clave Ks con la clave pública de un destinatario, la cual puede ser cargada en la memoria de la tarjeta protegida mediante una clave RSA. El destinatario puede descifrar la clave Ks usando la clave privada RSA correspondiente.

6. Cifrado

La tarjeta puede realizar operaciones 3 DES CBC con claves de 16 bytes (k1, k2, k1). Para realizar operaciones 3DES en la tarjeta, la clave de 16 bytes de longitud debe ser cargada en memoria. El proceso de carga está protegido por algoritmo RSA. La clave permanece en memoria hasta que se finaliza la sesión con la tarjeta o se carga una nueva.

Aplicaciones de firma

Uno de los principales usos del DNI electrónico es la realización de firma electrónica. Para utilizar esta funcionalidad de firma, numerosas aplicaciones pueden ser empleadas, ya que éstas acceden a las capas o módulos intermedios de CSP y PKCS#11, que proporcionan un interfaz estándar de acceso a la tarjeta.

Es recomendable seguir los consejos y buenas prácticas que se describen en la dirección http://www.dnielectronico.es/Asi_es_el_dni_electronico/consejos.html

Requisitos de seguridad del entorno

Para el correcto y seguro funcionamiento de la tarjeta DNle se han de utilizar los módulos criptográficos CSP y PKCS#11 que se encuentran en la dirección <http://www.dnielectronico.es/descargas/index.html>

Estos módulos contienen lo necesario para establecer un entorno seguro en la operación con el DNI electrónico y satisfacer los requisitos de seguridad aplicables al entorno de las tecnologías de la información descritos en el perfil de protección CWA 14169.

7. Servicio de Atención al Ciudadano



El DNI electrónico dispone de un Servicio de Atención al Ciudadano, con las siguientes características:

- Prestado de forma **permanente** (24 horas al día, 7 días a la semana).
- De ámbito **universal** (para todo tipo de usuarios).
- De modo **integral** (atiende cualquier tipo de incidencia del DNI electrónico).
- De forma **única** (sirve a todas las Autoridades de Validación).

El Servicio de Atención al Ciudadano es prestado por la Fábrica Nacional de Moneda y Timbre – Real Fábrica de la Moneda y puede accederse:

- Por teléfono: **902.364.444**
- Por correo electrónico: sac@dnielectronico.es

GLOSARIO DE TÉRMINOS. DEFINICIONES

Activación: es el procedimiento por el cual se desbloquean las condiciones de acceso a una clave y se permite su uso. En el caso de la tarjeta del DNLe 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 DNLe.

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 DNle.

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 DNle, 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 DNle: 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 DNle (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 DNle.

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

-o0o-



ANEXO

APLICACIÓN DE FIRMA

Como se ha comentado anteriormente, uno de los principales usos del DNI electrónico es la realización de firma electrónica. Para utilizar esta funcionalidad de firma, numerosas aplicaciones pueden ser empleadas, ya que éstas acceden a las capas o módulos intermedios de CSP y PKCS#11, que proporcionan un interfaz estándar de acceso a la tarjeta.

En el presente anexo se describe el manual de uso de una aplicación de firma que, si bien no es única y exclusiva para la operación con el DNLe, a la fecha es la referencia para la realización de firma electrónica con la tarjeta DNLe.

Las operaciones facilitadas por esta aplicación son:

- Firma: firma de un archivo, generando un nuevo fichero de firma.
- Firma documento adjunto: firma de un archivo, generando un nuevo fichero de firma, que contiene los datos firmados.
- Verificación off-line: comprobación de un archivo firmado con documento adjunto, en este tipo de verificación únicamente se comprueba si el certificado con el que ha firmado esta o no caducado, si el fichero firmado ha sido modificado y si el certificado de firma pertenece a una entidad de certificación de confianza.
- Verificación off-line sin documento adjunto: comprobación de un archivo firmado, en este tipo de verificación únicamente se comprueba si el certificado con el que ha firmado esta o no caducado y si el fichero firmado ha sido modificado, con respecto a un archivo facilitado por el usuario de la aplicación o mediante la inclusión de datos en un espacio facilitado por la aplicación.
- Verificación on-line: comprobación de un archivo firmado con documento adjunto. Comprende la verificación off-line y la comprobación del estado del certificado vía OCSP.
- Verificación on-line sin documento adjunto: comprobación de un archivo firmado. Comprende la verificación off-line sin documento adjunto y la comprobación del estado del certificado vía OCSP.

Todas y cada una de estas funciones soportarán firma múltiple.

Tanto los ficheros de firma resultantes como los de entrada a las operaciones de verificación seguirán el estándar CMS.



Hay que señalar que el usuario es el responsable final de utilizar la funcionalidad de firma en un sistema de creación de firma electrónica que garantice el cumplimiento de las garantías que exigen la Ley 59/2003 de firma electrónica y la directiva de firma electrónica (1999/93/CE), para su consideración como firma electrónica reconocida. Tales sistemas y aplicaciones son los homologados por la Dirección General de la Policía, con certificación del CCN.

Por otra parte, los sistemas y aplicaciones antes mencionados han de cumplir los siguientes requisitos:

- La aplicación de generación de firma electrónica debe realizar el hash de los datos a ser firmados por el DNle utilizando el algoritmo SHA-1
- La aplicación de generación de firma debe iniciar las comunicaciones con la tarjeta DNle, a tal objeto, bajo un canal seguro (se proporciona esta posibilidad) que proporcione integridad y confidencialidad de los datos enviados y recibidos entre este sistema y el DNle

Contexto del sistema

La aplicación esta basada en:

- Módulos PKCS#11 (interfaz con dispositivo de firma) desarrollados por la FNMT-RCM.
- Herramientas software para la implementación de operaciones criptográficas.
- Servicio de verificación de certificados (OCSP) de la FNMT-RCM.

Para la ejecución del programa es necesario que el usuario tenga instalada la máquina virtual de java, en su versión 5 (JRE 1.5).

Acrónimos y abreviaturas

Acrónimo / Abreviatura	Termino expandido
PKCS#11	Public Key Certificate Standard Number 11
PKCS#7	Public Key Certificate Standard Number 7
CMS	Cryptographic Message Syntax
OCSP	Online Certificate Status Protocol
JCE	Java Cryptography Extensión



Interfaz general de usuario

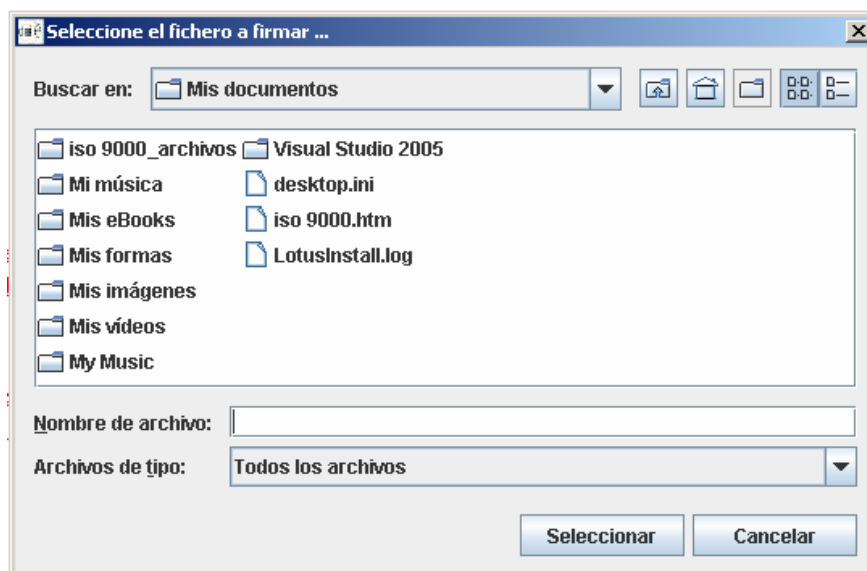
Aquí se describe la interfaz de usuario donde encontraremos acceso a todas las funcionalidades de la aplicación.



Esta primera interfaz de usuario da acceso a todas las funcionalidades de la aplicación, en este caso a las de firmar, verificar, configurar y a la ayuda.

Firma

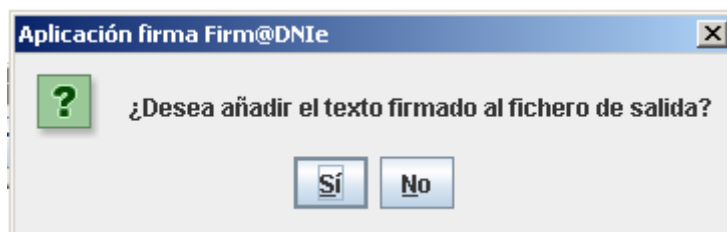
Cuando pulsemos en el botón de firmar, lo primero que se nos solicitará, es el fichero que deseamos firmar, para lo cual se nos muestra una pantalla como la siguiente:



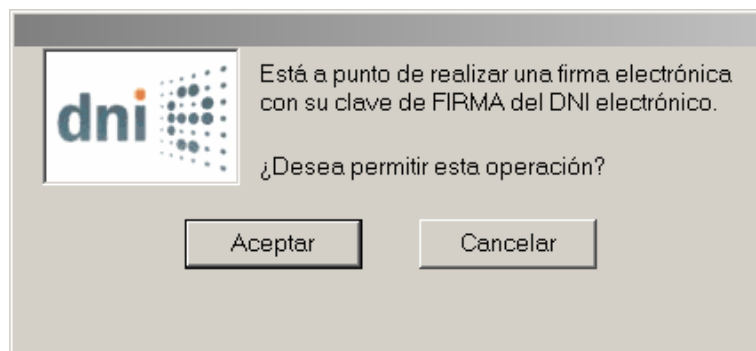
A continuación, tras seleccionar el fichero, se nos pide el código PIN



Si el código introducido es el correcto se nos pedirá una decisión para incluir o no lo firmado dentro de la propia firma generada, si es que sí, se generará un archivo que contiene lo firmado y la firma propiamente dicha



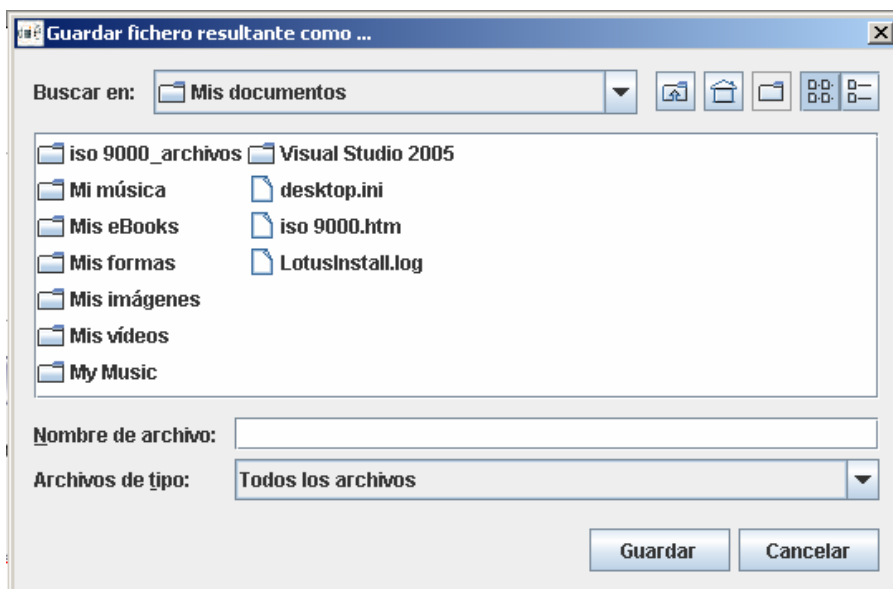
Posteriormente se nos pide autorización para realizar la operación



Finalmente se nos informa sobre el resultado de la operación



Y se nos pide el nombre del fichero en el que queremos almacenar el resultado



Se puede consultar una ayuda más detallada sobre este proceso en el menú de ayuda de la propia aplicación.

Verificación

En el proceso de verificación de un fichero firmado, mediante un cuadro de selección de ficheros, se nos solicitará la elección del mismo. Paso tras el cual se pedirá, si fuera necesario, el fichero original que se firmó. En este proceso no se requiere el código PIN del DNI electrónico, ya que la verificación se realiza mediante la clave pública del firmante del documento, no siendo necesario acceder en ningún caso a partes protegidas del DNI.

Pulsando el botón de "Verificar" se nos pide el fichero donde se encuentra la firma y en su caso los datos (si no estuviera en el mismo fichero, se nos solicitará el fichero de datos).



Una vez seleccionado el fichero, se nos muestra el resultado de la operación de forma gráfica y en la pantalla de resultados un detalle de la operación:

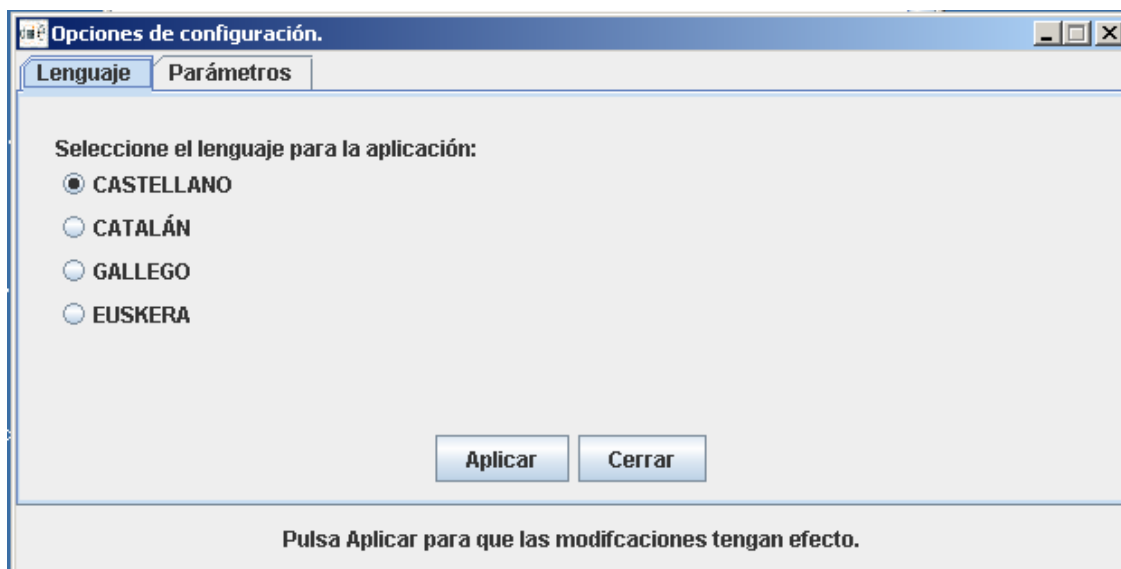


Puede encontrar más información sobre esta operación en la ayuda de la propia aplicación.

Configuración

La aplicación da la posibilidad de configurar una serie de parámetros como por ejemplo el lenguaje en el que se muestran los textos, etc.

El menú de configuración presenta el siguiente aspecto:



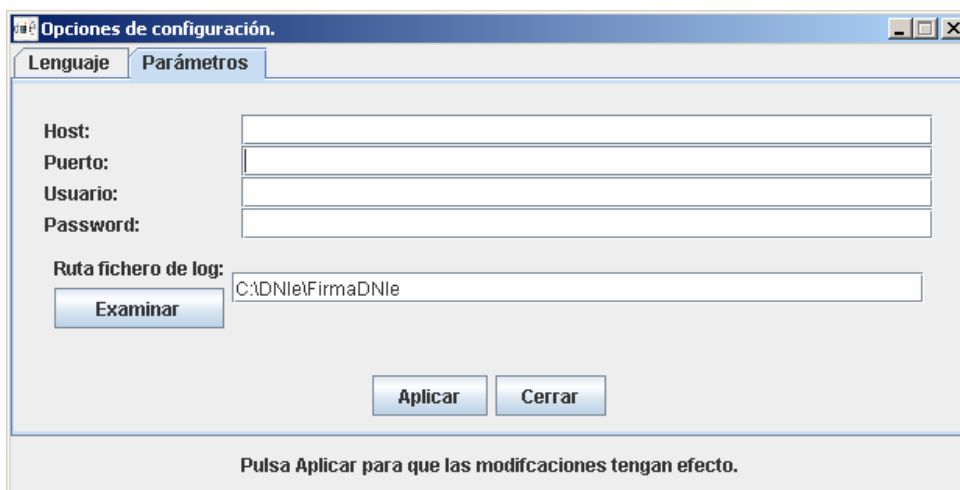
A través de las diferentes pestañas podremos ir accediendo a la configuración de los diferentes elementos que conforman la aplicación.

Es de especial interés la pestaña de parámetros en que se encuentran parámetros determinantes para el funcionamiento de la aplicación.

En primer lugar, si su ordenador tiene salida a la red pública a través de un Proxy que da servicio en un determinado puerto, ha de indicar su dirección y puerto en el campo "Host" y "Puerto" respectivamente

En el caso de que el proxy necesite autenticación con usuario y password se rellenarán los campos correspondientes.

Finalmente en el campo "Ruta de fichero de log" indicaremos el archivo donde queremos que la aplicación guarde un registro más detallado de su actividad.



Ayuda

La aplicación además ofrece una ayuda HTML que explica el funcionamiento del programa, y da una serie de nociones sobre criptografía.

La ayuda se presenta en el siguiente formato:

