

FORMACIÓN EN LÍNEA

**CENTRO DE RESPUESTA A INCIDENTES DE
SEGURIDAD (INTECO-CERT)**

ÍNDICE

1.	QUÉ ES EL DNI ELECTRÓNICO	4
1.1.	EN EL ANVERSO DE LA TARJETA	5
1.2.	EN EL REVERSO DE LA TARJETA	5
1.3.	QUÉ ES EL DNI ELECTRÓNICO: AUTOEVALUACIÓN	6
2.	VENTAJAS QUE APORTA EL DNI ELECTRÓNICO	7
2.1.	APLICACIONES	7
2.2.	SEGURIDAD	8
2.3.	UTILIZACIÓN (Ergonomía)	9
2.4.	VENTAJAS QUE APORTA EL NUEVO DNIE: AUTOEVALUACIÓN	11
3.	TECNOLOGÍA QUE INCLUYE EL NUEVO DNIE	12
3.1.	HARDWARE	12
3.2.	SOFTWARE	13
3.3.	CÓMO SE INSTALAN LOS MÓDULOS CRIPTOGRÁFICOS PARA EL DNIE	14
3.4.	TECNOLOGÍA QUE INCLUYE EL DNIE: AUTOEVALUACIÓN	22
4.	LEGISLACIÓN QUE REGULA EL DNIE ELECTRÓNICO	23
4.1.	MARCO LEGISLATIVO RELACIONADO CON EL DNI Y EL DNIE23	
4.2.	LEY 59/2003, de 19 de diciembre, de Firma Electrónica (BOE nº 304, 20/12/2003)	24
4.3.	LEGISLACIÓN COMPLEMENTARIA	26
4.4.	LEGISLACIÓN QUE REGULA EL NUEVO DNIE: AUTOEVALUACIÓN	29
5.	LOS CERTIFICADOS: QUÉ SÓN Y PARA QUÉ SIRVEN	30
5.1.	¿QUÉ ES UN CERTIFICADO?	32
5.2.	LOS CERTIFICADOS QUÉ SÓN Y PARA QUÉ SIRVEN: AUTOEVALUACIÓN	33
6.	LA FIRMA ELECTRÓNICA	34
6.1.	¿QUÉ ES LA FIRMA ELECTRÓNICA?	34

6.2.	LA FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN: aportando seguridad	36
6.3.	FIRMA DE TRÁMITES ADMINISTRATIVOS CON DNle	37
6.4.	LA FIRMA ELECTRÓNICA DEL DNle: las mayores garantías de seguridad	37
6.5.	LA FIRMA ELECTRÓNICA: AUTOEVALUACIÓN	38
7.	CUESTIONARIO DE AUTOEVALUACIÓN	39
8.	SOLUCIONES DEL CUESTIONARIO	42

1. QUÉ ES EL DNI ELECTRÓNICO

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

El DNI tradicional en sí es una cartulina plastificada. En él se recogían la fotografía del titular, ciertos datos del mismo y su firma manuscrita.



Con la llegada de la Sociedad de la Información y la generalización del uso de Internet, se plantea la necesidad de proporcionar a los ciudadanos una herramienta que les permita ampliar la utilización de su identidad al espacio digital, para poder realizar operaciones de comerciales y trámites administrativos.

Así, el nuevo DNI nace con la función de acreditar electrónicamente y de forma inequívoca la identidad de su titular o propietario.

El DNLe contiene la siguiente información:

1.3. QUÉ ES EL DNI ELECTRÓNICO: AUTOEVALUACIÓN

¿Cuál es la función del nuevo DNI?

- 1. Sustituir al antiguo DNI.
- 2. Acreditar la identidad de las personas sin dejar lugar a dudas.
- 3. Introducir más información en el DNI.

¿Qué novedad importante aporta el nuevo DNI?

- 1. El tipo de materiales de los que está hecho.
- 2. Que incluye un chip.
- 3. El hecho de que sirve para probar la identidad de forma electrónica, además de física

2. VENTAJAS QUE APORTA EL DNI ELECTRÓNICO

El DNI aporta ventajas en tres ámbitos diferentes:

APLICACIONES

El nuevo DNI ahorrará desplazamientos a las oficinas de la Administración Pública, con la comodidad de realizar trámites desde casa o el lugar de trabajo, mediante medios telemáticos

SEGURIDAD

El DNle incorpora mayores y más sofisticadas medidas de seguridad, que garantizan la confidencialidad de los trámites realizados por medios telemáticos

UTILIZACIÓN (Ergonomía)

Para facilitar su manejo y portabilidad, el DNle reúne una serie de características en esa línea: materiales de construcción, medidas, etc.

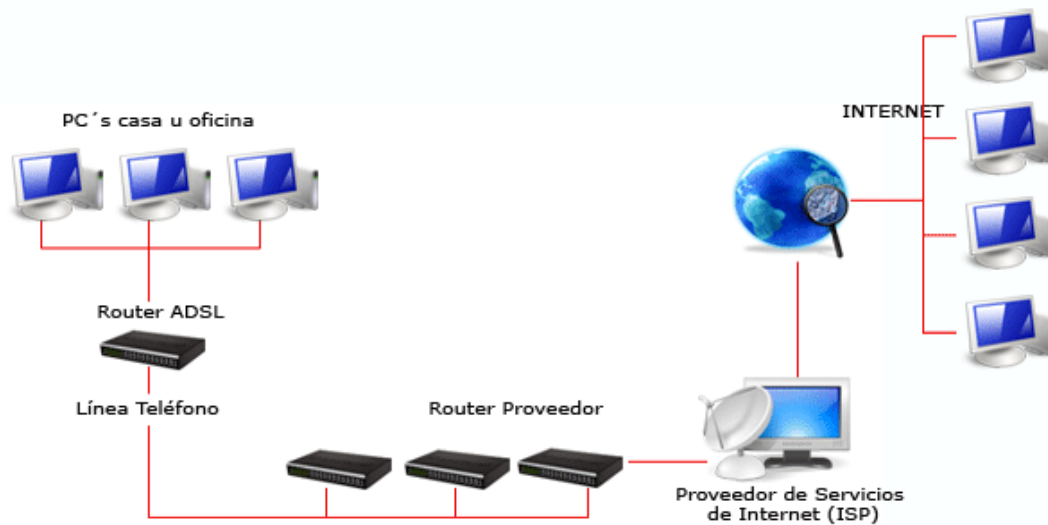
Veamos ahora en detalle cuáles son esas ventajas

2.1. APLICACIONES

Para cumplir con los nuevos retos de la Sociedad de la Información, el DNle permite:

- Relaciones con las empresas. En el ámbito de lo que se denomina **comercio electrónico** (también conocido como e-business) la utilización del DNI electrónico aporta **mayores niveles de seguridad** a los datos que se intercambian y proporciona a los que intervienen en la operación comercial **medidas que acreditan sus identidades**.
- Relaciones con las Administraciones Públicas. Ya sean estatales, autonómicas o locales, las administraciones van a facilitar a los ciudadanos la tramitación por vía telemática (e-government) **ahorrándoles muchos desplazamientos, simplificando las gestiones y con libertad de horarios**, todo ello con los niveles de seguridad y de garantía de acreditación de identidad necesarios.
- Relaciones entre ciudadanos y con la tecnología. La posibilidad de controlar el acceso a nuestro PC, o de poder entrar en edificios pasando nuestro DNle por un lector, o de intercambiar datos entre ciudadanos de igual forma que con la Administración o las empresas privadas, todo ello con medidas de seguridad y de autenticación de las partes.

En los tres casos, el medio telemático utilizado por excelencia es **Internet**.








Internet es un **conjunto de redes de ordenadores y equipos informáticos unidos** físicamente mediante cables, o a través de satélite o mediante servicios como la telefonía celular, que **conectan puntos de todo el mundo**. En cierto modo, no hay mucha diferencia entre Internet y la red telefónica que todos conocemos.

El acceso a los diferentes ordenadores y equipos informáticos que están conectados a Internet, puede ser público o estar limitado. En Internet, las comunicaciones concretas se establecen entre dos puntos: uno es el ordenador personal (en casa, en el trabajo) desde el que uno accede y el otro es cualquiera de los equipos informáticos que están conectados a Internet y facilitan información y servicios.

2.2. SEGURIDAD

Como hemos visto, cuando se utilizan medios telemáticos, es decir, sin presencia física de las personas que intervienen en la transacción, sea esta un trámite con la Administración Pública o una operación comercial con una empresa privada, hay una serie de factores que tener en consideración.

	Hay que comprobar	la identidad de los que intervienen.	AUTENTIFICACIÓN
	Hay que garantizar	la privacidad de la información.	CONFIDENCIALIDAD
	Hay que vigilar	que los datos no sean modificados.	INTEGRIDAD
	Hay que procurar	que las partes no se desdigan.	NO REPUDIO
	Hay que buscar	la validez legal de los documentos generados.	VALOR PROBATORIO

El Nuevo D.N.I dispone de un chip electrónico en el que se registran los datos del titular:

- Datos de filiación del titular
- Imagen digitalizada de la fotografía
- Imagen digitalizada de la firma manuscrita
- Certificado reconocido de autenticación y de firma
- Certificado electrónico de la autoridad emisora
- Par de claves de cada certificado electrónico

Es la información que contiene en su chip la que permite:

- Identificar y autenticar al titular
- Conocer sus datos de filiación
- Disponer de su firma manuscrita
- Poder firmar digitalmente formularios y otros documentos



2.3. UTILIZACIÓN (Ergonomía)

Con el fin de dar cabida al chip y a otras medidas, el soporte tradicional del DNI (cartulina plastificada) es sustituido por una tarjeta de policarbonato (un material plástico) con 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).

Esto quiere decir que no se notará el cambio al llevarla encima, ya que puede caber en las carteras, monederos, etc., en el mismo lugar en el que ya llevaba el DNI tradicional.



2.4. VENTAJAS QUE APORTA EL NUEVO DNIE: AUTOEVALUACIÓN

¿Cuál de estas es una ventaja que aporta el nuevo DNI?

- 1. Poder realizar trámites con la Administración sin salir de casa.
- 2. Evitar el robo del DNI.
- 3. Realizar pagos en el extranjero.

¿Cómo se denomina a garantizar la privacidad de la información en una transacción telemática?

- 1. No repudio.
- 2. Integridad.
- 3. Confidencialidad.

¿Cuáles de estos datos no se almacenan en el chip del DNIE, en formato digital?

- 1. Huella dactilar.
- 2. Iris del ojo.
- 3. Firma manuscrita.

3. TECNOLOGÍA QUE INCLUYE EL NUEVO DNIE

Elementos necesarios para utilizar el Dnie

Si se quiere utilizar el DNIE desde el hogar o desde el negocio, va a ser necesario disponer de una serie de tecnología, cada una con propósito y objetivo específicos.

3.1. HARDWARE

Se denomina así al equipamiento informático físico en general. Para el DNIE, se requieren dos cosas:

- 1. Un ordenador personal o PC.

El requisito es que sea de tecnología a partir de Intel Pentium III (esta tecnología se lanzó en el año 1999) o similar (el equivalente o superior de Pentium III en Celeron, Xeon u otros).



Es recomendable consultar con el vendedor del material informático para asesorarse del cumplimiento de los requisitos

- Un lector de tarjetas inteligentes (el DNIE se encuentra en esta categoría de tarjetas).

Estos lectores se presentan de diversas formas: puede venir integrado en el teclado del PC, o bien puede ser externo, que se conecten al ordenador a través de un puerto USB o de un interfaz PCMCIA.

Los requisitos que debe cumplir un lector de tarjetas para operar con el DNIE son los siguientes:

- Que cumpla con el estándar ISO 7816 (1,2, y 3). Este es el estándar para las tarjetas inteligentes.
- Que soporte tarjetas asíncronas basadas en los protocolos T=0 y T=1.
- Que soporte velocidades de comunicación mínimas de 9600 bps.

- Que soporte los estándares: API PC/SC (Personal Computer/Smart Card), CSP (Cryptographic Service Provider) y API PKCS#11



Es recomendable consultar con el vendedor del material informático para asesorarse del cumplimiento de los requisitos

3.2. SOFTWARE

Si se quiere utilizar el DNIe desde el hogar o desde el negocio, va a ser necesario disponer de una serie de tecnología, cada una con propósito y objetivo específicos.

Se denomina así a los programas informáticos de todo tipo que funcionan en los ordenadores personales o PC.

Sistemas operativos

El DNI electrónico puede operar en diversos entornos:

- Microsoft Windows (Win. XP, Win. 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 interaccionar 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.

Además de lo anterior, para operar con el lector de tarjetas será necesario instalar un "driver" (normalmente, se distribuye con el propio lector).

Driver: también llamado controlador de dispositivo o simplemente controlador. Es un programa informático que permite al sistema operativo interactuar con un periférico (periféricos son una impresora, una pantalla o, en este caso, un lector de tarjetas inteligentes)

- 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 **PKCS#11** específico para el DNI electrónico podrán obtenerse en el [Área de Descargas del Portal Oficial del DNI electrónico](#).

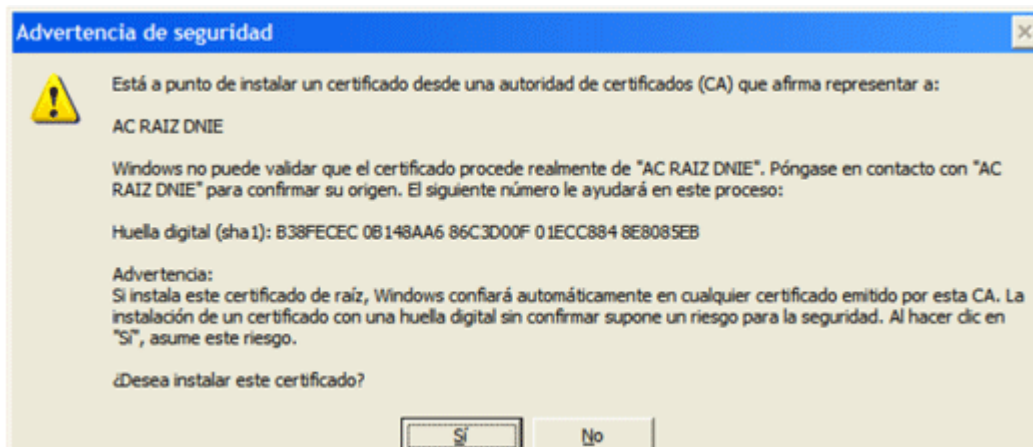
3.3. CÓMO SE INSTALAN LOS MÓDULOS CRIPTOGRÁFICOS PARA EL DNIE

ENTORNOS WINDOWS

- En el Área de Descargas del Portal Oficial del DNIE se encuentra el software con el ejecutable para la instalación del citado modulo criptográfico. El enlace es: http://www.dnielectronico.es/descargas/DNIEv2_5_2.zip (el número de versión puede cambiar).
- Con solo ejecutar este fichero se instalará el módulo CSP para el entorno Microsoft Windows y el módulo PKCS#11 para navegadores Firefox Mozilla y Netscape.
- Es necesario reiniciar el PC para finalizar la instalación. En el reinicio se instalará el Certificado Raíz de la DGP en los navegadores que estén instalados. También se configuran los dispositivos de seguridad de los navegadores Firefox Mozilla y Netscape instalados.
- En el directorio C:\DNIE se ubican dos ficheros para futuras configuraciones por parte del usuario:
 - Certificado raíz de la DGP:
CRAIZ_CERTIFICATE_AND_CRL_SIGNING_SHA1.crt
 - Módulo PKCS#11 para la instalación: **instalac.htm**
- En función de la configuración del navegador, es posible que cuando se reinicie el PC, aparezca la pantalla siguiente:



- Se solicitará que se confíe/instale el certificado raíz del DNIE, se deberá aceptar/instalar. Este paso es necesario para el correcto funcionamiento del DNIE.
- Se lanzará el "Asistente para importación de certificados". Hacer clic en "**Siguiente**".
- Dejar marcada la opción "**Seleccionar automáticamente el almacén de certificados en base al tipo de certificado**". Pulsar en "Siguiente" para continuar.
- Aparecerá un mensaje indicando que se ha completado con éxito la importación del certificado. Hacer clic en "**Finalizar**".
- Aparecerá una advertencia de seguridad, pulsar sobre el botón "**Sí**" para permitir que la autoridad raíz del DNIE, **AC RAIZ DNIE**, se instale en el navegador y de esta forma se pueda establecer adecuadamente la cadena de confianza de certificación.

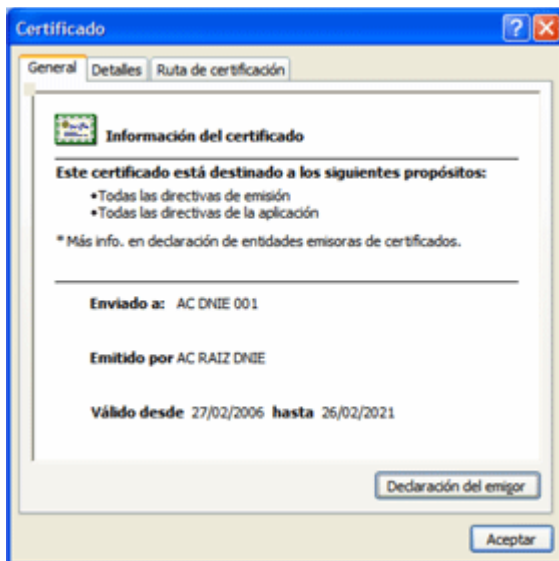


- Para ello debemos acceder al "Almacén de certificados" de cada uno de los navegadores instalados. En el caso de Internet Explorer, haríamos lo siguiente:
- A través del menú **Herramientas / Opciones de Internet / Contenido / Certificados...**

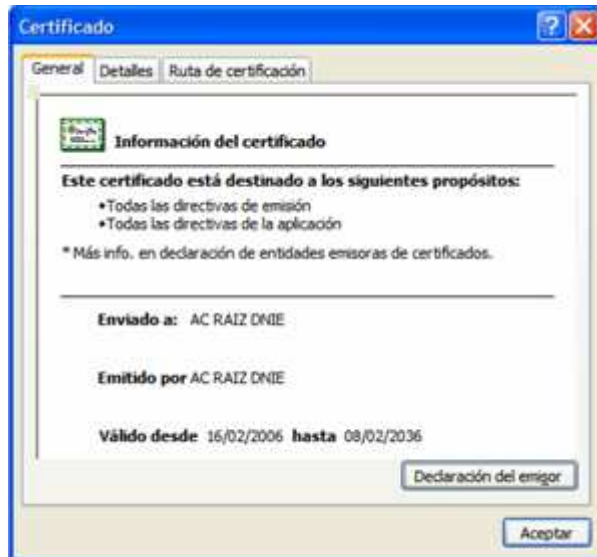


Si está instalado correctamente el módulo CSP (Proveedor de servicios de Certificación):

En la pestaña Entidades Emisoras de Certificados Intermedios podrá visualizar el certificado de autoridad intermedia AC DNIE 00X



En la pestaña Entidades emisoras raíz de confianza podrá visualizar el certificado raíz AC RAIZ DNIE.



ENTORNOS UNIX / LINUX O MAC

- El manual que describe los pasos necesarios para instalar y configurar las librerías de **OpenSC-DNIE** en entornos UNIX lo podemos encontrar en el Área de Descargas del Portal Oficial del DNI electrónico en el enlace: http://www.dnielectronico.es/descargas/PKCS11_para_Sistemas_Unix/install_opensc_dnie.pdf
- Distribuciones soportadas:
 - GNU/Linux Debian Etch
 - GNU/Linux Ubuntu Dapper Draker
 - GNU/Linux Ubuntu Edgy Eft
 - GNU/Linux Ubuntu Feisty Fawn
 - GNU/Linux Ubuntu Gutsy Gibbon
 - Fedora Core 5
 - Mac OS X
 - Solaris 10
 - X86
 - SPARC

¿CÓMO COMPROBAR QUE FUNCIONA MI DNI ELECTRÓNICO?

Una vez tenemos instalados y configurados todos los elementos hardware y software requeridos, ya estamos en condiciones de poder utilizar el DNI electrónico.

- **Existen dos posibilidades para verificar su funcionamiento:**

1. Se puede comprobar su correcto funcionamiento y consultar los datos que han sido almacenados en el chip, en los Puntos de Actualización del DNle (PAD)* existentes en las Oficinas de Expedición.
2. Desde cualquier PC que disponga de un lector de tarjetas criptográficas y tenga instalados los drivers de acceso, podrá consultar los certificados almacenados en el chip del DNI electrónico.

A continuación detallamos los pasos a realizar en este caso:

Notas: * **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.).

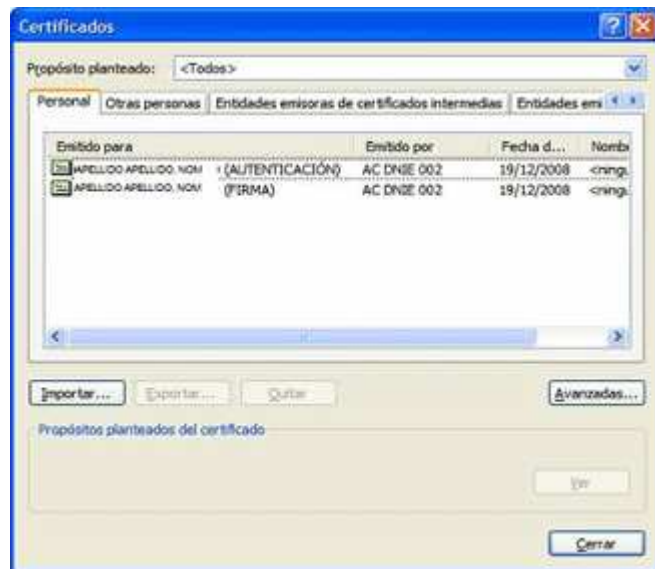
VERIFICAR FUNCIONAMIENTO DESDE UN PC

- Introducir el DNle correspondiente en el lector de tarjetas.
- Abrir un navegador. En este ejemplo hemos utilizado "Internet Explorer". Para otros navegadores, Mozilla Firefox, Netscape, etc., el procedimiento es similar aunque varía la forma de acceder al "Almacén de certificados".
- Seleccionamos las siguientes opciones del menú por este orden: "Herramientas" >> "Opciones de Internet" >> "Contenido" >> "Certificados"
- En este momento el navegador accederá al contenedor de certificados entre los cuales estarán los certificados del DNle, por lo que para poder acceder a los mismos se nos presenta una ventana en la que se solicita la introducción del PIN* del DNle.



Notas: * **Clave Personal de Acceso (PIN):** Secuencia de caracteres que permiten el acceso a los certificados. El código PIN es personal e intransferible, por tanto, únicamente debe ser conocido por el titular de la tarjeta en cuestión. Se genera aleatoriamente en el momento de expedición del DNI y se entrega al ciudadano en forma de sobre ciego.

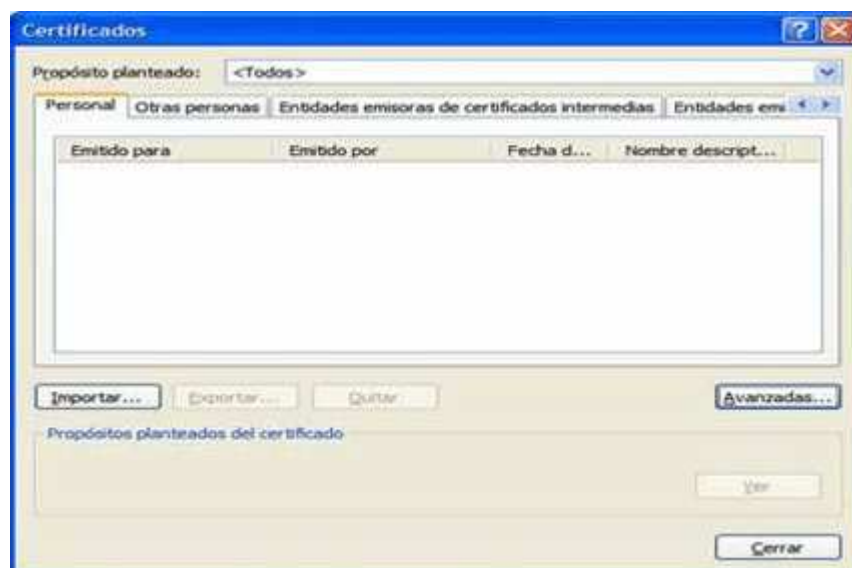
- Una vez introducido el PIN correcto se mostrarán los dos certificados del DNIe (el de autenticación y el de firma) en la pestaña "Personal".



Para ver los detalles de cada uno, debemos hacer doble "clic" o pulsar el botón "Ver" habiendo seleccionado cualquiera de ellos.

COMPROBACIÓN DEL BLOQUEO DEL PIN

- Si hemos realizado correctamente cada uno de los pasos anteriores y no se muestran los certificados en el navegador, puede ser que el PIN del documento haya sido bloqueado.



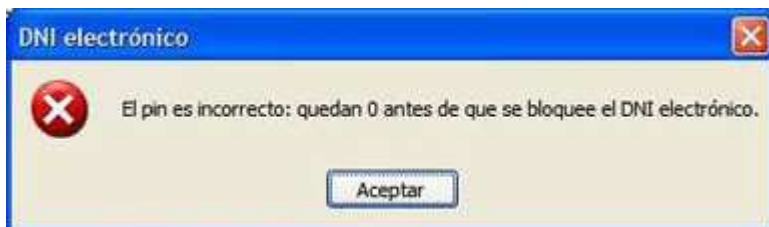
- Cuando el PIN ha sido bloqueado anteriormente aunque éste se introduzca correctamente no serán mostrados los certificados en la ventana del navegador, ya que no se pueden acceder a ellos por el bloqueo.

Para comprobarlo haremos lo siguiente:

- Con el DNle en el lector, abrir el navegador "Windows Internet Explorer" y seleccionar las siguientes opciones del menú por este orden: "Herramientas" >> "Opciones de Internet" >> "Contenido" >> "Certificados".
- Se nos presenta la ventana en la que se solicita la introducción del PIN del DNle.

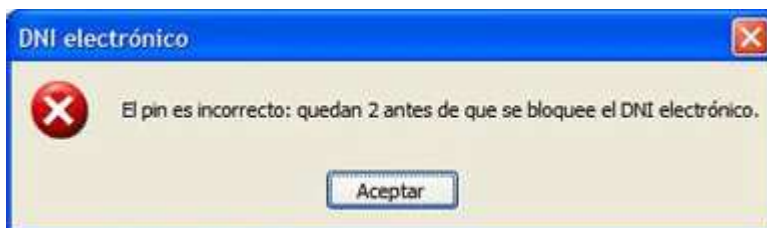


- En esta ventana **SE DEJA LA CASILLA DEL PIN EN BLANCO** (importante no introducir ningún carácter) y se selecciona "**Aceptar**", de esta forma se nos informará del número de intentos que nos quedan antes de que se bloquee el PIN.



- Al realizar esta acción **NO SE DESCUENTAN INTENTOS** se descuentan intentos del estado actual del mismo, seguiremos teniendo el mismo número de ellos y además nos permitirá conocer si se encuentra bloqueado o aún es operativo.

Se descontará un intento cada vez que se introduzca el PIN incorrectamente.



- Si antes de ser bloqueado se pone correctamente una vez el PIN, el contador se reseteará y volverá a la situación ideal (**3 intentos**).
- En caso de bloqueo del PIN la única solución posible para desbloquearlo es acudir a una oficina de expedición del DNle y hacer uso de un **Punto de Actualización del DNle** que le permitirá hacer un cambio de PIN de forma segura tras una correcta presentación de la huella dactilar del usuario, que actuará de código de desbloqueo.

AUTENTICACIÓN A TRAVÉS DEL DNIE

- Una vez que hemos verificado la correcta instalación y funcionamiento de los elementos necesarios para la utilización del DNI electrónico, podemos hacer uso de cualquiera de los servicios disponibles como se indica en http://www.dnielectronico.es/servicios_disponibles/
- Cuando establezcamos una conexión con una página Web de un Organismo Público (o una Entidad Privada) que requiera una autenticación a través del DNle por parte del usuario, será necesario tener nuestro DNle insertado en el lector de tarjetas criptográficas.
- El navegador nos mostrará una nueva ventana con el listado de certificados que tengamos instalados y estén admitidos por el servidor.
- Se deberá seleccionar el certificado de AUTENTICACIÓN de nuestro DNle.
- Durante el proceso se solicitará que introduzcamos el PIN (en ocasiones más de una vez).
- El Organismo Público (o la Entidad Privada) comprobará, a través de la Autoridad de Validación, el estado de validez de nuestro certificado de autenticación.
- Si el proceso de autenticación finaliza correctamente, se habrá establecido un canal seguro de comunicación entre ambas partes.

3.4. TECNOLOGÍA QUE INCLUYE EL DNIE: AUTOEVALUACIÓN

¿Cuál de estos elementos no es necesario para utilizar el DNI electrónico desde un PC?

- 1. Un lector de tarjetas inteligentes.
- 2. Una pantalla en color.
- 3. El o los "drivers" para el lector de tarjetas.

Si su PC tiene instalado un sistema operativo Windows, ¿qué servicio debe tener instalado?

- 1. CSP.
- 2. PKCS #11.
- 3. Firefox.

Si el PIN de acceso a los certificados de su DNI electrónico se ha bloqueado, ¿qué debe hacer?

- 1. Llamar a la comisaría más próxima.
- 2. Acudir a un Punto de Actualización del DNIE.
- 3. Solicitar un nuevo DNI.

4. LEGISLACIÓN QUE REGULA EL DNIE ELECTRÓNICO

4.1. MARCO LEGISLATIVO RELACIONADO CON EL DNI Y EL DNIE



El artículo 9 de la **Ley Orgánica 1/1992, de 21 de Febrero, sobre Protección de la Seguridad Ciudadana**, expone el derecho de todos los españoles a que se les expida el DNI, que además será obligatorio a partir de los catorce años.



El artículo 12.1 de la **Ley Orgánica 2/1986, de 13 de Marzo, de Fuerzas y Cuerpos de Seguridad**, adjudica a la Policía Nacional la función de la expedición del DNI.



Es la **Ley Orgánica 59/2003, de 19 de Diciembre, de Firma Electrónica***, la que regula, fijando su marco normativo, respecto del **documento nacional de identidad electrónico**, que se erige en un certificado electrónico reconocido, llamado a generalizar el uso de instrumentos seguros de comunicación electrónica, capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos.

Esta ley introduce una serie de conceptos que deben conocerse. Vamos a verlos a continuación.

** Que tiene una base en la 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.*

4.2. LEY 59/2003, de 19 de diciembre, de Firma Electrónica (BOE nº 304, 20/12/2003)

UN BREVE RESUMEN

Artículo 1. Objeto.

1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

Artículo 4. Empleo de la firma electrónica en el ámbito de las Administraciones Públicas.

1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.(...)
2. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.



Artículo 15. Documento nacional de identidad electrónico.

1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.
2. Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico (...)

Artículo 19. Declaración de prácticas de certificación.

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación (...)

2. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación de protección de datos de carácter personal (...)

Artículo 29. Supervisión y control.

1. El Ministerio de Industria, Turismo y Comercio controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados electrónicos de las obligaciones establecidas en esta ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica.

Artículo 24. Dispositivos de creación de firma electrónica.

2. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

- a. Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
- b. Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.
- c. Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
- d. Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma..

CONCEPTOS DEFINIDOS EN LA LEY 59/2003

- **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.
- **Firma electrónica avanzada:** 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.
- **Firma electrónica reconocida:** 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.
- **Prestador de servicios de certificación (PSC):** persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- **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.
- **Certificados reconocidos:** certificados electrónicos expedidos por un PSC que cumpla los requisitos establecidos la Ley 59/2003 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.

4.3. LEGISLACIÓN COMPLEMENTARIA

Real Decreto 1553/2005, de 23 de Diciembre, por el que se regula la expedición del DNI y sus certificados de firma electrónica



Establece que el DNle es el instrumento para la identificación electrónica de su titular, además de con él pueda realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, cuya firma electrónica realizada a través de tal DNI tendrá respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel.

Actualmente, conviven el DNI "clásico" con el DNI electrónico, en el que están activados los certificados electrónicos. Esta activación tendrá carácter voluntario y se llevará a cabo mediante una clave personal secreta. Para llevar a cabo la activación, se exige mayoría de edad y plena capacidad de obrar.

El periodo de validez del DNI es distinto del de sus certificados electrónicos. El del DNI es, salvo supuestos especiales, de cinco años, diez años o sin plazo (permanente). Los certificados electrónicos tienen una vigencia de treinta meses, y al expirar este plazo, puede solicitarse la expedición de un nuevo certificado electrónico reconocido, manteniendo el mismo DNI mientras éste continúe vigente, para cuya solicitud debe mediar presencia física del titular. Si no se procede a tal renovación del certificado, éste se incluirá en la lista de los revocados.

En otro orden, indica que todos los españoles tendrán derecho a que se les expida el Documento Nacional de Identidad, siendo obligatoria su obtención por los mayores de catorce años residentes en España y para los de igual edad que, residiendo en el extranjero, se trasladen a España por tiempo no inferior a seis meses.

También fija la obligación de exhibir el DNI a todas las personas que están obligadas a obtener el Documento Nacional de Identidad, cuando fueren requeridas para ello por la autoridad o sus agentes.

Ley 11/2007, de 22 de Junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)

"...La Ley consagra la relación con las Administraciones Públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones. El reconocimiento de tal derecho y su correspondiente obligación se erigen así en el eje central del proyecto de Ley.

De forma general, es una ley que pretende reglamentar todos aquellos aspectos relacionados con el procedimiento administrativo para permitir que éste sea llevado a cabo en un contexto electrónico; fundamentalmente, tratando de eliminar todos aquellos aspectos recogidos en el ordenamiento administrativo "clásico" (Ley de Procedimiento Administrativo 17 de julio de 1958, Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, Ley 4/1999,...)

Las implicaciones de dicha Ley afectan de modo general a la práctica totalidad de las actividades de las Administraciones Públicas."

Ley 56/2007, de 28 de Diciembre, de medidas de Impulso a la Sociedad de la Información (LISI)

Artículo 2. Obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica.

1. [...] las empresas que presten servicios al público en general de especial trascendencia económica **deberán facilitar** a sus usuarios **un medio de interlocución telemática** que, mediante **el uso de certificados reconocidos de firma electrónica**, les permita la realización de, al menos, los siguientes trámites:

Ley 56/2007, de 28 de Diciembre, de medidas de Impulso a la Sociedad de la Información (LISI)

- a. Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.
- b. Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.
- c. Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.

- d. Ejercicio de sus derechos ARCO en los términos previstos en la normativa reguladora de protección de datos de carácter personal.

2. [...] tendrán la consideración de empresas que presten servicios al público en general de especial trascendencia económica, las que agrupen a **más de cien trabajadores o su volumen anual de operaciones**, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, **exceda de 6.010.121,04 euros** y que, en ambos casos, **operen en** los siguientes sectores económicos:

- a. Servicios de comunicaciones electrónicas a consumidores, en los términos definidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
- b. **Servicios financieros destinados a consumidores**, que incluirán los servicios bancarios, de crédito o de pago, los servicios de inversión, las operaciones de seguros privados, los planes de pensiones y la actividad de mediación de seguros.

4.4. LEGISLACIÓN QUE REGULA EL NUEVO DNIE: AUTOEVALUACIÓN

¿La firma electrónica reconocida tiene el mismo valor que la firma manuscrita?

- 1. Si.
- 2. No.
- 3. A veces.

¿Es obligatorio para todos los españoles tener el DNI?

- 1. Si.
- 2. No.
- 3. Sólo para los mayores de catorce años, con las condiciones que marca la ley.

¿Qué es un PSC?

- 1. Un organismo público.
- 2. Un prestador de servicios de certificación.
- 3. La política de servicios de certificación que establecen las empresas.

5. LOS CERTIFICADOS: QUÉ SÓN Y PARA QUÉ SIRVEN

Hasta ahora, se han visto y repetido conceptos tales como “**certificado electrónico**” y “**firma electrónica**”

pero, ¿qué son? ¿Cómo funcionan? Y, sobre todo, ¿cuáles son las ventajas que aportan? También se ha mencionado que el DNle contiene dos certificados: uno para autenticar la identidad del ciudadano y otro para que este firme de forma electrónica cualquier tipo de transacción telemática.

No hay que olvidar que, en el mundo de la tecnología y las comunicaciones electrónicas, como es el de Internet, hay varios riesgos que deben tenerse presentes y ser conscientes de ellos, para poderlos evitar:

- Asegurar que **sólo el emisor y el receptor de cualquier mensaje vean la información transmitida (confidencialidad)**
- Verificar que el mensaje no ha sido manipulado por el camino (**integridad**)
- Confirmar la identidad del emisor y del receptor de la información transmitida (**autenticación**)



Ya desde la antigüedad, se han empleado métodos para garantizar que el contenido de un mensaje intercambiado entre dos personas, sólo pudiese ser leído e interpretado correctamente por ellas.

El primer método conocido se debe a Julio Cesar. Su sistema, denominado de sustitución, consistía en reemplazar en el mensaje a enviar cada letra por la situada tres posiciones por delante en el alfabeto latino.

Se llama **Criptografía** a la técnica de transformar un mensaje inteligible, denominado **texto en claro**, en otro que sólo puedan entender las personas autorizadas a ello, que será el **texto cifrado**. El método o sistema empleado para cifrar el texto en claro se denomina **algoritmo de cifrado**.

El siguiente paso fue el uso de una palabra o serie determinada como base de un sistema de cifrado. Este sistema posee la ventaja de que, si el sistema es complejo, tan sólo será fácil obtener el texto en claro a quién sepa dicha palabra, además de ser fácil de recordar.

Esta palabra o serie base del mecanismo de cifrado se denomina **clave de cifrado**, y el número de letras que la forman se llama **longitud de la clave**.

Indudablemente, cuanto más complicado sea el mecanismo de cifrado y cuanto más larga sea la clave, más difícil será romper el sistema y obtener el mensaje original para un extraño.



Las claves son la base fundamental de los modernos sistemas criptográficos, basados en operaciones matemáticas generalmente muy complejas.

Básicamente, los algoritmos de cifrado se pueden clasificar en dos:

1) **Simétricos**, denominados de **clave privada**, que utilizan la misma clave para cifrar y descifrar el texto claro.

Este sistema presentaba un gran inconveniente. El emisor tiene que generar muchas claves distintas (para que ningún receptor pueda descifrar mensajes que el emisor envía a otros receptores) y eso le supone un gran esfuerzo.

Por ello, se creó otro sistema mucho más seguro.

2) **Asimétricos**, denominados de **clave pública**, en los que existen dos claves. Una cifra el texto claro y la otra lo descifra.

La clave privada del emisor NUNCA es conocida por otras personas.

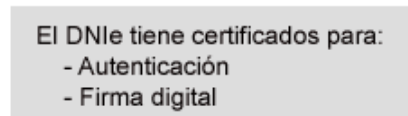
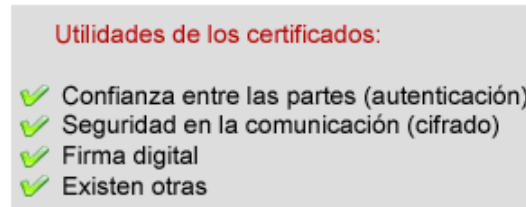
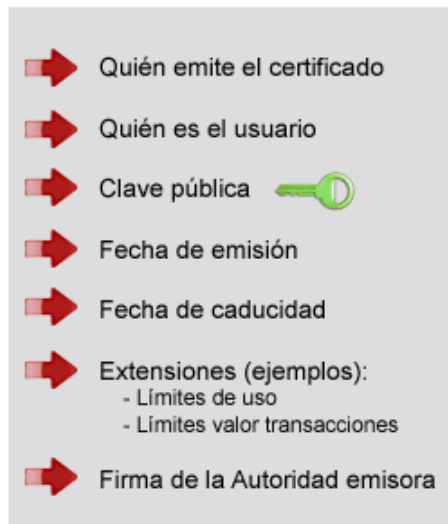
Así, cuando el receptor descifra un mensaje con la clave pública del emisor, tiene certeza de que el mensaje viene de quien dice que viene.

Además, ya se está garantizando la confidencialidad del mensaje, ya que sólo el emisor y el receptor van a conocer su contenido.

Ahora bien, para dar aún más garantías de la procedencia del mensaje y de la integridad del mismo, los métodos criptográficos crearon la FIRMA DIGITAL, que se verá en el capítulo siguiente.

5.1. ¿QUÉ ES UN CERTIFICADO?

Un certificado es un documento firmado electrónicamente que autentica la relación de una clave (privada o pública) con un usuario (en el caso del DNle, con un ciudadano).



En el DNI electrónico, se utiliza el sistema de clave pública o asimétrico.

Cuando un ciudadano acude a una oficina de expedición del DNIE, seguirá una serie de pasos (un protocolo de actuación) en el que se incluye la generación de los certificados.

Es imprescindible la presencia física de la persona que solicitar la expedición del DNle.

La generación de las dos claves (de autenticación y de firma) y sus correspondientes certificados, se realizará en la tarjeta del DNle y en presencia del titular solicitante, tras la habilitación de un PIN* aleatorio que se le entrega personalmente en un sobre ciego.

*Un PIN es un código formado por una combinación de letras y números, diferente al del resto de los titulares de DNle. Es una medida de protección similar a la que se utilizar en las tarjetas de crédito bancarias.

La entrega del Documento Nacional de Identidad y de los certificados asociados, se realizará personalmente a su titular en la misma jornada en que solicite su expedición.

5.2. LOS CERTIFICADOS QUÉ SÓN Y PARA QUÉ SIRVEN: AUTOEVALUACIÓN

¿Qué es un texto cifrado?

- 1. Un texto cuyo contenido es falso.
- 2. Un mensaje que se emite.
- 3. Un texto que sólo pueden entender las personas autorizadas para ello, porque poseen la clave para descifrarlo.

¿El DNI posee certificados con el propósito de cifrar información?

- 1. Si.
- 2. No, pero se pueden utilizar para ello.
- 3. No, posee uno para autenticación y otro para firma digital.

¿Cuál de estas es la ventaja del sistema de clave pública o asimétrica?

- 1. El emisor sólo tiene que intercambiar una misma clave con todos los receptores.
- 2. Se generan dos claves distintas.
- 3. No existen ventajas con el sistema de clave privada o simétrica.

6. LA FIRMA ELECTRÓNICA

En el mundo real, en nuestra vida diaria, es un acto bastante común el de estampar nuestra **firma manuscrita** en documentos variados.

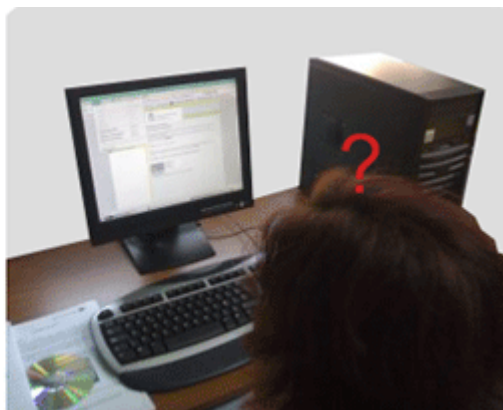
¿Cuál es el equivalente de esto en el mundo digital?

No hay que olvidar el artículo apartado 2 del artículo 1 del Real Decreto 1553/2005, de 23 de Diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, dice "Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignan, así como la nacionalidad española del mismo".

Esto se complementa con el apartado 1 del artículo 15 de la Ley de Firma Electrónica, que dice que

"El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos."

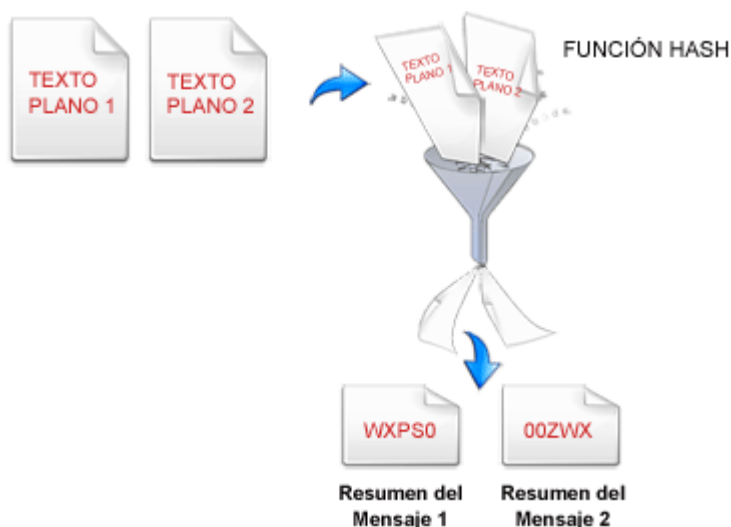
Por lo tanto, tenemos en el DNle el instrumento para realizar la firma electrónica de documentos digitales. Pero, ¿qué es la firma electrónica y en qué consiste? ¿cuáles son las ventajas que aporta?



6.1. ¿QUÉ ES LA FIRMA ELECTRÓNICA?

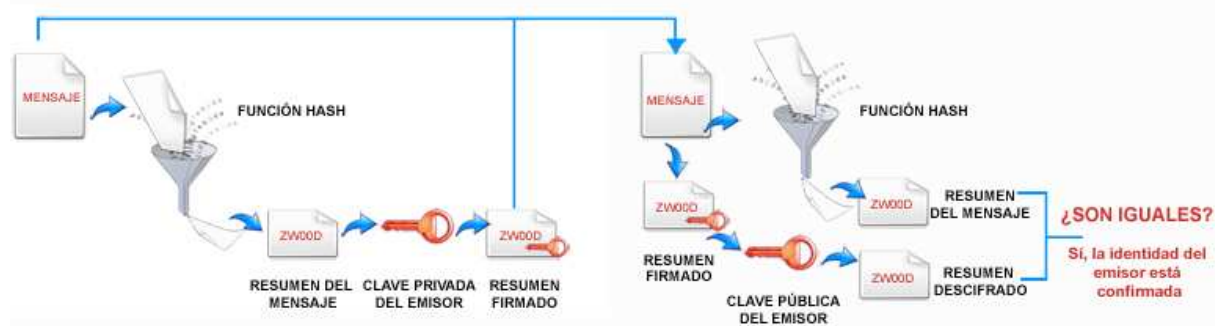
En matemáticas, existe una función llamada "hash" (significa "resumen"), que tiene unas características peculiares:

- Aplicada sobre un conjunto de datos (un mensaje de correo electrónico, por ejemplo), se obtiene otro nuevo conjunto de datos de tamaño fijo, más pequeño.
- Este nuevo conjunto de datos está asociado unívocamente a los datos iniciales, es decir, en nuestro ejemplo es imposible encontrar dos mensajes de correo electrónico que generen el mismo resultado al aplicarles una función hash.



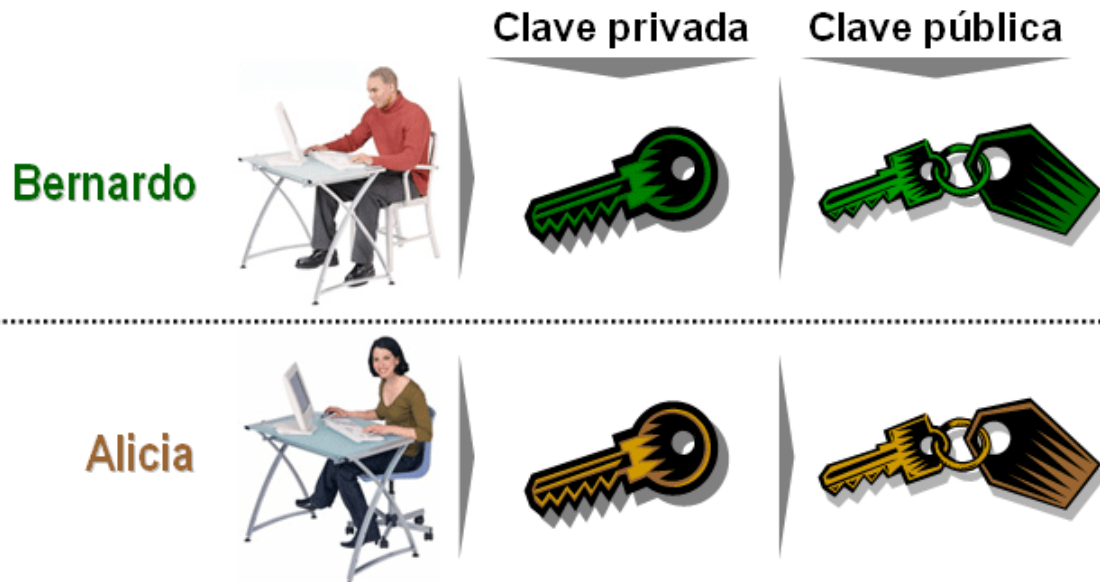
La **Criptografía** utiliza esto de la siguiente manera:

1. El emisor tiene un conjunto de datos (mensaje) que quiere enviar por medios telemáticos, por ejemplo: una transferencia a través de Internet, un correo electrónico, un formulario de compra, o cualquier otra cosa que requiera seguridad en el envío.
2. A los datos a firmar se le aplica un algoritmo basado en una función hash. Se obtiene un resumen del mensaje.
3. El emisor cifra ese resumen con su clave privada. Esta es la firma electrónica.
4. La firma electrónica se añade al mensaje y éste se envía.
5. El receptor recibe el mensaje y la firma (el resumen cifrado). Aplica la función hash de nuevo sobre el mensaje y obtiene un resumen. Descifra con la clave pública del emisor, el resumen que venía con el mensaje y entonces compara los dos resúmenes. Si ambos coinciden, la firma es válida.



6.2. LA FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN: aportando seguridad

Dos entidades pueden intercambiar información secreta sobre un canal inseguro garantizando la confidencialidad, la integridad y el no repudio.



Bernardo manda un mensaje cifrado y firmado a Alicia



Bernardo usa la clave pública de Alicia (que conoce todo el mundo) y su clave privada (que solo conoce él):



- **Cifra** el mensaje que manda a Alicia (confidencialidad) con la pública de Alicia.
- **Firma** el mensaje con su propia clave privada (integridad, no repudio).



Alicia usa su clave privada (que solo conoce ella) y la clave pública de Bernardo (que conoce todo el mundo):



- **Comprueba** la validez de la firma (integridad, no repudio) con la pública de Bernardo.
- **Desprotege** el mensaje que Bernardo le envía (confidencialidad) con su propia clave privada.

6.3. FIRMA DE TRÁMITES ADMINISTRATIVOS CON DNLe

(datos tomados del documento "DNI electrónico Guía de Referencia Básica", de la Comisión Técnica de Apoyo a la Implantación del DNI electrónico, el cual se encuentra a disposición de todos los ciudadanos en el sitio web www.dnielectronico.es)

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:

6.4. LA FIRMA ELECTRÓNICA DEL DNLe: las mayores garantías de seguridad

- La clave del certificado para la firma electrónica NUNCA sale del chip electrónico en el que se almacena dentro de la tarjeta del DNLe
- Los certificados y sus claves almacenados en el chip del DNLe, están PROTEGIDOS mediante un PIN, que se proporciona al ciudadano, en sobre cerrado, durante el acto de expedición del nuevo documento nacional de identidad. También se le proporciona a los ciudadanos la posibilidad de cambiar ese PIN a voluntad, en los denominados Puntos de Actualización del DNLe, ubicados en las Oficinas de Expedición del DNI
- Todo el proceso de generación de claves y certificados se hace EN PRESENCIA DEL CIUDADANO
- El certificado para firma electrónica que incluye el DNLe está considerado por la ley española como "firma electrónica avanzada". Esto quiere decir que TIENE EL MISMO VALOR sobre los datos consignados en forma electrónica que la firma manuscrita los tiene sobre los DATOS CONSIGNADOS EN PAPEL.
- El conjunto formado por el certificado de autenticación y el de firma permiten: GARANTIZAR LA IDENTIDAD del ciudadano, LA INTEGRIDAD de los documentos firmados electrónicamente y el NO REPUDIO.

¡¡ Atención !! No se debe utilizar NUNCA el certificado de autenticación para la firma electrónica de documentos

6.5. LA FIRMA ELECTRÓNICA: AUTOEVALUACIÓN

¿Cuál de estas propiedades no garantiza la firma electrónica?

- 1. Integridad.
- 2. No repudio.
- 3. Confidencialidad.

El certificado de firma electrónica que posee el DNle, está catalogado como...

- 1. De firma electrónica solamente.
- 2. De firma electrónica avanzada.
- 3. De firma electrónica reconocida.

¿En qué consiste la firma electrónica?

- 1. En aplicar una función matemática denominada hash a los datos.
- 2. En cifrar los datos con la clave privada.
- 3. En la combinación de aplicar la función hash a los datos y luego cifrar el resultado con la clave privada del emisor.

7. CUESTIONARIO DE AUTOEVALUACIÓN

Para finalizar, un sencillo cuestionario general para que Usted mismo pueda determinar qué grado de comprensión ha adquirido sobre la materia. Esto no es obligatorio. Simplemente, es una sencilla herramienta que ponemos a su disposición para ayudarle. En la siguiente página, encontrará una serie de preguntas generales sobre todos los aspectos del DNI electrónico vistos durante la formación. Por favor, conteste si lo desea.

1. ¿El nuevo Documento Nacional de Identidad, denominado DNI electrónico o DNLe, tiene la misma misión que el DNI tradicional. Ahora bien, ¿su ámbito de uso es idéntico?

- 1. Sí, sólo pueden utilizarse para identificar al ciudadano presencialmente.
- 2. No, hay que utilizar los dos documentos, tradicional y electrónico, uno para cada cosa.
- 3. No, con el DNLe también se acreditará la identidad de la persona electrónicamente, además de presencialmente.

2. Para ampliar su ámbito de uso, el DNLe incluye algún nuevo elemento que lo permite, ¿cuál es este nuevo elemento?

- 1. Un chip criptográfico.
- 2. Información impresa OCR-B para lectura mecanizada.
- 3. Tintas especiales.

3. ¿Cuál de las siguientes no es una ventaja del DNLe?

- 1. Incluye nuevos mecanismos para impedir su falsificación.
- 2. Funciona como una tarjeta monedero.
- 3. Sirve para que el ciudadano realice ciertos trámites electrónicos.

4. ¿Cómo definiría la autenticación?

- 1. La manera en la que una persona registra su identidad en un sistema.
- 2. La forma de asegurar la privacidad de la información.
- 3. El proceso de confirmar la identidad de algo o alguien (en el caso del DNLe, la de un ciudadano).

5. Una de las ventajas del DNle es que puede utilizarlo para hacer trámites, de forma electrónica, desde un PC. Pero para ello, ¿necesita disponer de algún elemento adicional?

- 1. No es necesario nada adicional.
- 2. Sólo debe disponer de un lector de tarjetas inteligentes, conectado al PC.
- 3. Son necesarios un lector de tarjetas inteligentes y una serie de software (módulo criptográfico y driver del lector de tarjetas) instalados en el PC.

6. Siempre que desde su PC quiera acceder a los certificados que almacena su DNle, ¿qué es lo que va a ocurrir?

- 1. Que se muestran normalmente en la pantalla de su PC.
- 2. Que se le va a solicitar que introduzca un PIN para autorizar el acceso a los certificados.
- 3. Que un programa le preguntará cuál de los certificados es el que quiere ver.

7. La legislación española otorga al DNle capacidad para acreditar electrónicamente la identidad personal de su titular y permitir la firma electrónica de documentos. ¿Qué ley es la que lo establece?

- 1. Ley Orgánica 1/1992, de 21 sobre Protección de la Seguridad Ciudadana.
- 2. La Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.
- 3. La Ley 59/2003, de Firma Electrónica, en su artículo 15.

8. ¿Cuál de estos tres tipos de firma electrónica tiene el mismo reconocimiento, desde un punto de vista legal, que la firma manuscrita?

- 1. La firma electrónica reconocida.
- 2. La firma electrónica avanzada.
- 3. Cualquier tipo de firma electrónica generada por una empresa en España.

9. ¿Cuál de estas características diferencia fundamentalmente el proceso de solicitud y generación del DNle frente al DNI tradicional?

- 1. Se digitalizan la fotografía y la huella dactilar del solicitante.
- 2. Se requiere la presencia física del solicitante en todo el proceso de generación.
- 3. Se utiliza un nuevo tipo de material para la tarjeta.

10. ¿Qué es un certificado?

- 1. Es el método por el que un texto en claro puede alterar su contenido para que no sea legible.
- 2. Es un mecanismo que relaciona una clave con su propósito de uso (cifrado, firma, etc.).
- 3. Es un documento firmado electrónicamente que autentica la relación de una clave con un usuario.

11. La firma digital es un mecanismo de garantía de...

- 1. Integridad y no repudio.
- 2. Confidencialidad.
- 3. Autenticación.

12. Los certificados que incluye el DNle ¿tienen una finalidad determinada?

- 1. No, se pueden utilizar indistintamente cualquiera de los dos.
- 2. Uno es para cifrado y otro para firma.
- 3. Uno es sólo para autenticación del ciudadano y otro es sólo para firma digital.

8. SOLUCIONES DEL CUESTIONARIO

QUÉ ES EL DNI ELECTRÓNICO: SOLUCIÓN

¿Cuál es la función del nuevo DNI?

2. Acreditar la identidad de las personas sin dejar lugar a dudas.

¿Qué novedad importante aporta el nuevo DNI?

3. El hecho de que sirve para probar la identidad de forma electrónica, además de física

VENTAJAS QUE APORTA EL NUEVO DNIE: SOLUCIÓN

¿Cuál de estas es una ventaja que aporta el nuevo DNI?

1. Poder realizar trámites con la Administración sin salir de casa.

¿Cómo se denomina a garantizar la privacidad de la información en una transacción telemática?

3. Confidencialidad.

¿Cuáles de estos datos no se almacenan en el chip del DNIE, en formato digital?

2. Iris del ojo.

TECNOLOGÍA QUE INCLUYE EL DNIE: SOLUCIÓN

¿Cuál de estos elementos no es necesario para utilizar el DNI electrónico desde un PC?

2. Una pantalla en color.

Si su PC tiene instalado un sistema operativo Windows, ¿qué servicio debe tener instalado?

1. CSP.

Si el PIN de acceso a los certificados de su DNI electrónico se ha bloqueado, ¿qué debe hacer?

2. Acudir a un Punto de Actualización del DNIE.

LEGISLACIÓN QUE REGULA EL NUEVO DNIE: SOLUCIÓN

¿La firma electrónica reconocida tiene el mismo valor que la firma manuscrita?

1. Si.

¿Es obligatorio para todos los españoles tener el DNI?

3. Sólo para los mayores de catorce años, con las condiciones que marca la ley.

¿Qué es un PSC?

2. Un prestador de servicios de certificación.

LOS CERTIFICADOS QUE SÓN Y PARA QUÉ SIRVEN: SOLUCIÓN

¿Qué es un texto cifrado?

3. Un texto que sólo pueden entender las personas autorizadas para ello, porque poseen la clave para descifrarlo.

¿El DNI posee certificados con el propósito de cifrar información?

3. No, posee uno para autenticación y otro para firma digital.

¿Cuál de estas es la ventaja del sistema de clave pública o asimétrica?

1. El emisor sólo tiene que intercambiar una misma clave con todos los receptores.

LA FIRMA ELECTRÓNICA: SOLUCIÓN

¿Cuál de estas propiedades no garantiza la firma electrónica?

3. Confidencialidad.

El certificado de firma electrónica que posee el DNle, está catalogado como...

2. De firma electrónica avanzada.

¿En qué consiste la firma electrónica?

3. En la combinación de aplicar la función hash a los datos y luego cifrar el resultado con la clave privada del emisor.

CUESTIONARIO DE AUTOEVALUACIÓN: SOLUCIÓN

1. ¿El nuevo Documento Nacional de Identidad, denominado DNI electrónico o DNle, tiene la misma misión que el DNI tradicional. Ahora bien, ¿su ámbito de uso es idéntico?

3. No, con el DNle también se acreditará la identidad de la persona electrónicamente, además de presencialmente.

2. Para ampliar su ámbito de uso, el DNle incluye algún nuevo elemento que lo permite, ¿cuál es este nuevo elemento?

1. Un chip criptográfico.

3. ¿Cuál de las siguientes no es una ventaja del DNle?

2. Funciona como una tarjeta monedero.

4. ¿Cómo definiría la autenticación?

3. El proceso de confirmar la identidad de algo o alguien (en el caso del DNle, la de un ciudadano).

5. Una de las ventajas del DNle es que puede utilizarlo para hacer trámites, de forma electrónica, desde un PC. Pero para ello, ¿necesita disponer de algún elemento adicional?

3. Son necesarios un lector de tarjetas inteligentes y una serie de software (módulo criptográfico y driver del lector de tarjetas) instalados en el PC.

6. Siempre que desde su PC quiera acceder a los certificados que almacena su DNle, ¿qué es lo que va a ocurrir?

2. Que se le va a solicitar que introduzca un PIN para autorizar el acceso a los certificados.

7. La legislación española otorga al DNle capacidad para acreditar electrónicamente la identidad personal de su titular y permitir la firma electrónica de documentos. ¿Qué ley es la que lo establece?

3. La Ley 59/2003, de Firma Electrónica, en su artículo 15.

8. ¿Cuál de estos tres tipos de firma electrónica tiene el mismo reconocimiento, desde un punto de vista legal, que la firma manuscrita?

1. La firma electrónica reconocida.

9. ¿Cuál de estas características diferencia fundamentalmente el proceso de solicitud y generación del DNle frente al DNI tradicional?

2. Se requiere la presencia física del solicitante en todo el proceso de generación.

10. ¿Qué es un certificado?

3. Es un documento firmado electrónicamente que autentica la relación de una clave con un usuario.

11. La firma digital es un mecanismo de garantía de...

1. Integridad y no repudio.

12. Los certificados que incluye el DNle ¿tienen una finalidad determinada?

3. Uno es sólo para autenticación del ciudadano y otro es sólo para firma digital.