

Administración de Sistemas y Seguridad
Máster Profesional en Ingeniería Informática
Universidad de Granada
Curso académico 2018-2019



**UNIVERSIDAD
DE GRANADA**

Certificados Digitales

DNI ELECTRÓNICO

Correa Fernández, Gema 75572158-T
gcorrea@correo.ugr.es

Toda la información del trabajo se encuentra en:
https://github.com/Gecofer/MII_ASS_1819

28 de mayo de 2019

Índice

1. Certificado digital	1
1.1. ¿Qué es el certificado digital o certificado electrónico?	1
1.2. ¿Qué son las claves digitales?	2
1.3. Formato de los certificados digitales	2
1.4. Tipos de certificados digitales	3
2. DNI electrónico	6
2.1. Componentes del DNI electrónico	7
2.1.1. Chip criptográfico	8
2.2. Seguridad en el DNI electrónico	9
2.3. ¿Que ventajas nos ofrece el DNI electrónico?	9
2.4. ¿Cómo utilizar el DNI electrónico?	10
2.5. Diferencias entre DNI-e y DNI 3.0	11
3. Firma electrónica	13
3.1. ¿Qué es la firma electrónica?	13
3.2. ¿A qué nos referimos con firma digital?	13
3.2.1. Ejemplo de implementación firma digital	15
4. Conclusiones	19

1. Certificado digital

Imaginemos una situación cotidiana: *una persona en un establecimiento desea pagar sus compras con su tarjeta de crédito*. Para ello, dicha persona debe firmar un documento en el que da su conformidad a que se le descuento de su cuenta el importe gastado. Pero, ¿cómo puede estar seguro el responsable del establecimiento de que el qué firma es el propietario de la tarjeta? Normalmente, el responsable pide el **DNI** a dicha persona, para así comprobar la identidad del firmante. Por tanto, para verificar dicha identidad, se recurre a un documento que asegura que esa persona es quién dice ser. Puesto que en ese documento confiamos, ya que confiamos en la entidad que ha emitido el DNI (Dirección General de Policía, Ministerio del Interior). Es decir, para verificar a la persona ha habido que recurrir a una tercera parte, en quien se confía, y que asegura que la persona no está mintiendo acerca de su identidad.

Si pasamos esto al mundo de las comunicaciones digitales, la situación que se acaba de plantear es muy similar: si alguien firma un documento con una firma digital, ¿cómo puede convencer a quién lo recibe de que la firma la ha realizado esa persona? Se puede comprobar que esa firma se ha realizado con una determinada clave privada, pero ¿corresponde esa clave privada con quién dice realizar la firma? Aquí es donde entra lo que se conoce como una tercera parte de confianza, es decir, algo o alguien en quien confían tanto el firmante como el que recibe la firma. Esa tercera parte de confianza, emite un **certificado digital** (también llamado certificado electrónico) que no es más que un documento digital en el que se relaciona una identidad con unos datos, y que va firmado digitalmente por quién lo emite.

1.1. ¿Qué es el certificado digital o certificado electrónico?

Un **certificado digital** o **certificado electrónico** es un documento que identifica a una persona (física o jurídica) con un par de claves. Es expedido por una Autoridad de Certificación, es decir, está firmado electrónicamente por un prestador de servicios de certificación¹, considerado por otras entidades como una autoridad que vincula unos datos de verificación de firma a un firmante. El certificado digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet.

El objetivo de este certificado es validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta, siendo un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de la red. Tiene una estructura de datos que contiene información necesaria para firmar electrónicamente e identificar a su firmante con sus datos. Para ello, todo certificado digital debe tener:

- Información relativa al propietario del certificado.
- Información relativa al emisor del certificado.
- Claves del propietario.
- Firma digital del certificado por el emisor.

¹Se denomina prestador de servicios de certificación, la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Por tanto, el certificado permite la firma electrónica de documentos: *el receptor de un documento firmado puede tener la seguridad de que éste es el original y no ha sido manipulado y, el autor de la firma electrónica no podrá negar la autoría de esta firma.* Asimismo, la autoridad de certificación da fe de que la firma electrónica se corresponde con un usuario concreto. Además, la firma de la estructura de datos agrupa la información que contiene, de forma que no pueda ser modificada sin que ésta modificación sea detectada.

1.2. ¿Qué son las claves digitales?

Un certificado digital consta de una pareja de **claves criptográficas**, es decir, una **clave pública** y una **clave privada**, creadas con un algoritmo matemático, esenciales para la firma e identificación del firmante. Ambas claves trabajan de forma complementaria, esto es, lo que cifra o codifica una clave sólo lo puede descifrar o decodificar la otra. La diferencia entre ellas es que la clave privada está pensada para que nunca salga del certificado y esté siempre bajo el control del firmante. En cambio, la clave pública se puede repartir o enviar a otros usuarios o entidades.

Por esta razón, se puede concluir que la clave pública forma parte de lo que se denomina certificado digital en sí, ya que dicho certificado contiene la clave pública junto con los datos del titular, y firmado electrónicamente por una Autoridad de Certificación.

Por otra parte, el dueño del certificado debe mantener siempre la clave privada bajo su control, ya que si ésta es sustraída, se podría suplantar la identidad del titular en la red. En este caso, el sujeto debería revocar el certificado lo antes posible, del mismo modo que si anulásemos una tarjeta de crédito.

1.3. Formato de los certificados digitales

```

1 Certificate:
2 Data:
3 Version: 3 (0x2)
4 Serial Number: 9 (0x9)
5 Signature Algorithm: sha1WithRSAEncryption
6 Issuer: C=US, ST=Florida, L=Tampa, O=Text CA,
7 CN=bsd.jcs.local
8 Validity
9 Not Before: Mar 31 20:02:42 2003 GMT
10 Not After : Mar 30 20:02:42 2004 GMT
11 Subject: C=US, ST=Florida, L=Tampa, O=sslecho,
12 CN=linux.jcs.local
13 Subject Public Key Info:
14 Public Key Algorithm: rsaEncryption
15 RSA Public Key: (1024 bit)
16 Modulus (1024 bit):
17 00:d6:6f:d6:40:00:8a:c6:86:00:b8:31:62:f3:06:
18 bd:c1:f0:10:b5:b9:34:8c:f7:d6:09:98:66:9d:dd:
19 a5:90:5e:58:fb:06:9d:59:21:75:fb:ac:ab:86:56:
20 83:57:a0:f8:55:1e:53:90:45:f7:e9:3f:66:b1:f3:e7:
21 fd:59:c1:88:ee:86:13:3c:79:55:c9:50:58:ae:5a:
22 32:d5:0e:aa:a7:f0:fd:2c:88:b9:89:1c:9d:3e:95:
23 27:6b:cc:a9:1f:5e:c0:99:d5:65:79:1e:2d:64:d3:
24 63:dd:99:8f:1f:22:1d:2f:2e:1b:f9:39:6c:c5:1e:
25 b3:01:00:1a:07:56:21:5b:c3
26 Exponent: 65537 (0x10001)
27 X509v3 extensions:
28 Netscape Cert Type:
29 SSL Server
30 Signature Algorithm: sha1WithRSAEncryption
31 4b:e7:22:94:f9:09:c3:db:6b:a5:c3:ea:39:b7:9a:04:36:c9:
32 de:d7:c2:ed:59:d7:bb:b9:4c:ec:35:04:15:e9:32:d6:b0:ea:
33 d8:64:5d:5c:41:3f:bb:c9:41:c7:32:fd:ad:47:52:20:c4:d5:
34 04:3a:92:ab:59:f8:34:3c:57:bd:cc:15:ac:f4:3e:59:11:3f:
35 c4:3f:2f:a5:7f:ef:89:8f:13:51:e6:9c:a7:94:20:71:ed:5a:
36 1d:57:65:bb:38:34:2f:0a:86:73:e2:18:e0:8f:23:4d:d0:63:
37 37:b6:ee:0f:44:07:1d:94:66:70:78:ef:31:d1:97:50:11:ec:
38 25:c3

```

Figura 1: Ejemplo de un certificado X.509

En la figura 1 podemos ver un ejemplo de un certificado X.509. El **formato X.509** es el más común de los certificados digitales. Es un conjunto estándar de campos con información referente al usuario y al emisor. Está definido por el estándar internacional *ITU-T X.509*, de esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con dicho estándar. Existen 3 versiones de dicho certificado: la primera de 1988, la segunda de 1993 y la tercera de 1996. Los certificados X.509 deben contener los siguientes campos:

Versión	Especifica la versión del estándar X.509 que se ha empleado (puede ser la 1, la 2 o la 3).
Número de serie	Cada vez que una entidad crea un certificado se debe asociar un número de serie, que no puede repetir en otro certificado.
Algoritmo de firma	Especifica el algoritmo que ha usado el emisor para firmar el certificado.
Entidad emisora	Nombre de la entidad que emite el certificado.
Periodo de validez	Por seguridad, los certificados tienen un tiempo de vida: se indica cuando comienza a ser válido y cuando dejará de serlo.
Datos del sujeto	Datos identificativos del dueño del certificado.
Clave pública del sujeto	La clave pública del dueño del certificado, y el algoritmo asociado.
ID único de la entidad emisora	Una cadena de bits que se usa para identificar a la entidad emisora.
ID único del sujeto	Una cadena de bits que se usa para identificar al dueño.
Extensiones	Información adicional permitida por el estándar.
Firma digital de la entidad emisora	Firma de todos los campos anteriores del certificado, realizada con la clave privada de la entidad emisora.

En España la entidad que más certificados digitales ha emitido es la **Fábrica Nacional de Moneda y Timbre (FNMT)**, a través de la autoridad pública de Certificación Española (CERES).

1.4. Tipos de certificados digitales

La obtención del certificado digital depende de si el certificado está contenido en una tarjeta, como el DNI-e, o de si el certificado se guarda en un fichero software. No obstante, para ambos casos se debe de identificar al propietario del mismo, lo que requiere que dicha persona se presente en las oficinas de una Autoridad de Registro, para corroborar su identidad. Prácticamente, todas las webs que requieran de certificado funcionan tanto con uno como con otro (ver figura 4).

Entonces, podemos concluir que distinguimos dos tipos de certificados, principalmente:

1. El **certificado contenido en una tarjeta**, como el **DNI-e** o DNI electrónico, que se incluye en el chip del DNI.
2. El **certificado software emitido por la Fábrica Nacional de Moneda y Timbre (FNMT)**.

Si se desea obtener el certificado que incluye el DNI electrónico lo único que se necesita es el carnet de identidad, ya que en ese momento se proporciona un sobre con el PIN del DNI-e. Por el contrario, si se decide utilizar los certificados del DNI electrónico se deberá adquirir un lector de tarjetas y renovar los certificados en el tiempo estipulado. Para el caso de los certificados software emitidos por la FNMT, el PIN no será necesario una vez se haya instalado, ya que es el propio navegador del usuario quién crea las claves.

A partir de estas principales diferencias, podemos destacar las siguientes disimilitudes entre el DNI electrónico y los certificados software.

Características del certificado digital

La solicitud y descarga del certificado se realizan desde el navegador. Se debe de utilizar el mismo navegador durante todo el proceso, desde la solicitud hasta la descarga final del certificado.
Se instala en el navegador web en soporte fichero o soporte software, utilizando la extensión .p12 o .pfx.
Cada proceso de solicitud depende de cada Autoridad de Certificación.
Sólo funciona en los equipos en los que haya sido instalado, pero existe la posibilidad de exportar los certificados a otros equipos.
La caducidad de cada certificado depende de la FNMT o de la Autoridad de Certificación, con una media de tres años (36 meses).



Gema Correa
Fernandez.p12

Figura 2: Mi certificado digital emitido por la FNMT

Emitido para	
Nombre común (CN)	CORREA FERANDEZ GEMA - 75572158T
Organización (O)	
Unidad organizativa (OU)	
Número de serie	[REDACTED]
Emitido por	
Nombre común (CN)	AC FNMT Usuarios
Organización (O)	FNMT-RCM
Unidad organizativa (OU)	Ceres
Periodo de validez	
Comienza el	6 de mayo de 2019
Caduca el	6 de mayo de 2023
Huellas digitales	
Huella digital SHA-256	[REDACTED]
Huella digital SHA1	[REDACTED]

Figura 3: Información acerca de mi certificado digital

Características del DNI electrónico
Al caducar el Documento Nacional de Identidad, también extinguirán su validez los certificados incorporados en el DNI-e.
A diferencia del certificado software, la firma electrónica con DNI-e sí es considerada como firma electrónica reconocida, ya que en este caso se trata de un dispositivo de creación de firmas seguro.
Se necesita un lector de tarjetas en el caso de que se desee utilizar el DNI electrónico, sin embargo, el lector no será necesario, si se posee el nuevo DNI 3.0 ya que incorpora la tecnología NFC.
Obtener estos certificados es gratis, pero en el caso de renovación o pérdida del DNI-e, se tendrá que pagar un coste.
Su duración suele ser de 30 meses, y para solicitar uno nuevo deberemos hacerlo presencialmente, con o sin renovación del DNI.



Figura 4: Pedir cita de atención primaria en el SAS

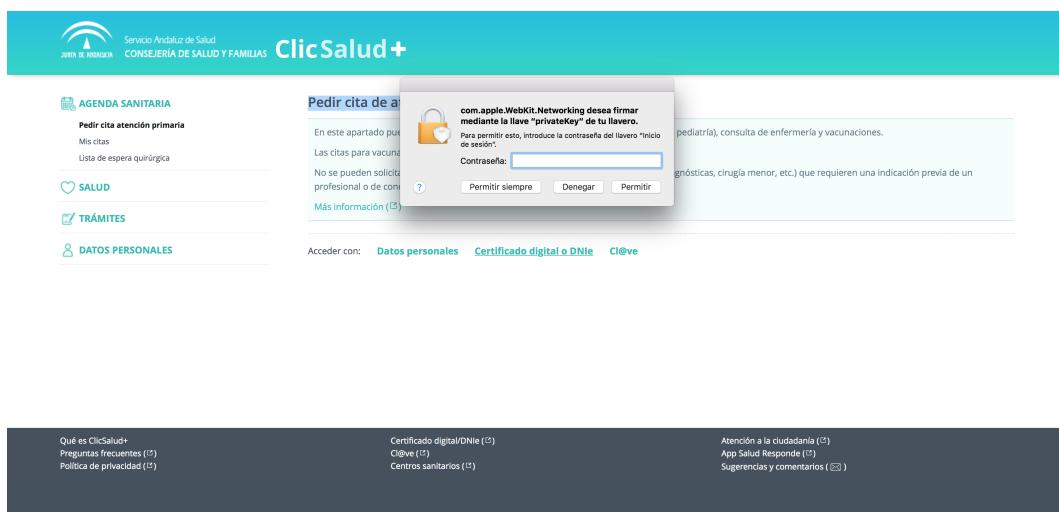


Figura 5: Acceso mediante certificado software (introducir contraseña)



Figura 6: Acceso completado

En definitiva, independientemente del certificado que se adquiera, disponer de un certificado permitirá ahorrar tiempo y dinero al realizar trámites administrativos en Internet, a cualquier hora y desde cualquier lugar.

2. DNI electrónico

El **DNI electrónico** es un documento emitido por la Dirección General de la Policía (Ministerio del Interior) y no sólo sirve para confirmar la identidad de una persona concreta, sino para:

- Acreditar electrónicamente y de forma inequívoca la identidad de la persona.
- Realizar firmas digitales en documentos electrónicos, otorgándoles de la misma validez jurídica que con la firma tradicional.



Figura 7: DNI electrónico

Adicionalmente, el DNI-e incorpora un pequeño **circuito integrado** (chip), que contiene los mismos datos que aparecen impresos en la tarjeta (datos personales, fotografía,

firma y huella dactilar digitalizada) junto con los certificados de Autenticación y de Firma Electrónica. La importancia del certificado en el DNI electrónico reside en el chip que contiene (ver figura 7), gracias a él, podemos obtener los certificados:

- **Certificado de Autenticación:** tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática, asegurando que la comunicación electrónica se realiza con la persona que dice que es. Así, 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.
- **Certificado de Firma:** tiene como finalidad permitir al ciudadano firmar trámites o documentos. Permite sustituir la firma tradicional por la electrónica en las relaciones del ciudadano con terceros.

De esta forma, cualquier persona podrá realizar múltiples gestiones online de forma segura con las Administraciones Públicas, con empresas públicas y/o privadas, y con otros ciudadanos, a cualquier hora y sin tener que desplazarse ni hacer colas.

2.1. Componentes del DNI electrónico

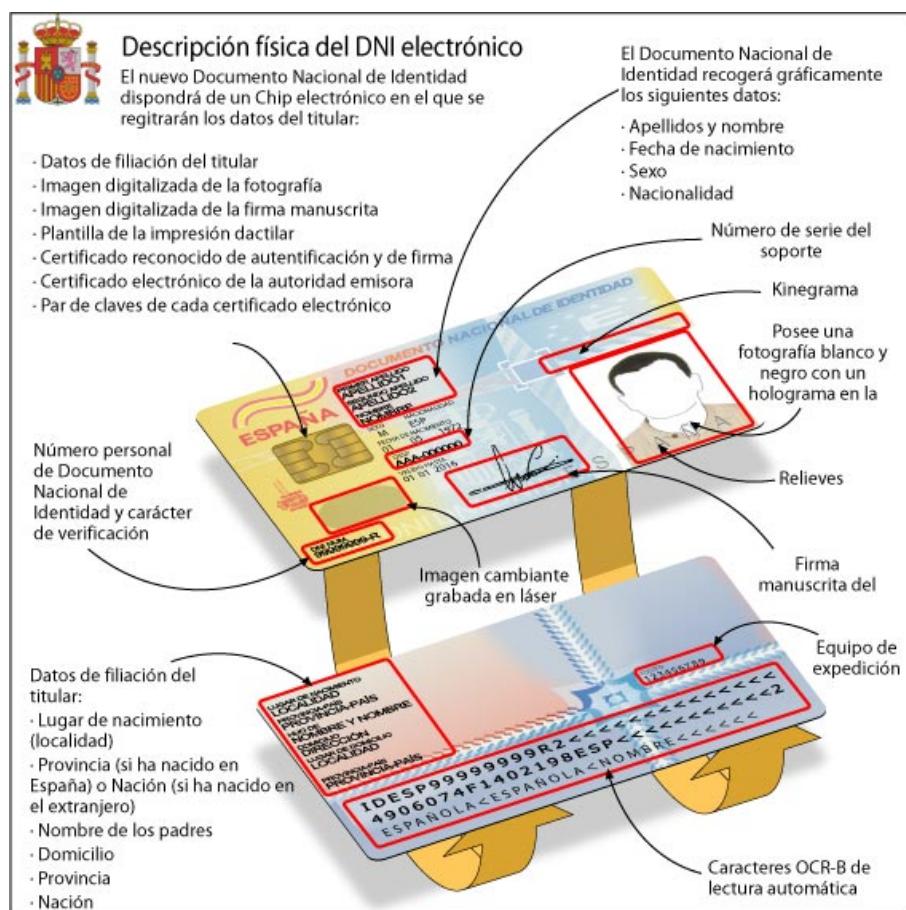


Figura 8: Descripción física del DNI-e

Como bien sabemos, el DNI electrónico es una tarjeta de plástico, que incorpora un chip con información digital y que tiene unas dimensiones idénticas a las del DNI tradicional (85,60 mm de ancho X 53,98 mm de alto). En la figura 8, se observan sus principales componentes. Su validez es de 30 meses (menos de 3 años), siendo renovables por el ciudadano en una oficina de expedición. Se utiliza para firmar electrónicamente SHA-1 y usa claves RSA.

2.1.1. Chip criptográfico

El chip del DNI está localizado en la parte central izquierda del anverso del Documento de Identidad Nacional. Este chip permite dotarlo de la capacidad de ser leído de forma rápida y sencilla por las máquinas, no por las personas. Como se ha comentado, incorpora parte de los mismos datos que aparecen impresos en la tarjeta:

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

Respecto a las características del chip, mencionar que contiene el sistema operativo DNIe v1.1 con una capacidad de información de 32KB. Además, dicha información está clasificada en zonas diferentes según su accesibilidad:

- **Zona pública**, accesible en lectura sin restricciones, contiene la Autoridad de Certificación, que es la entidad responsable de emitir el certificado, claves *Diffie-Hellman*, que es un protocolo criptográfico para compartir claves y formato X.509 para el certificado (*visto anteriormente*).
- **Zona privada**, accesible en lectura por el ciudadano mediante una Clave Personal de Acceso o PIN, y contiene los Certificados de Autenticación y de Firma.
- **Zona de seguridad**, accesible en lectura por el ciudadano en los puntos de actualización del DNI. Contiene los datos de filiación del ciudadano contenidos en el soporte físico del DNI, la imagen de la fotografía digitalizada y la imagen de la firma manuscrita (digitalizada).

En lo referente a la estructura de la clave pública para el DNI, se asignan las funciones de Autoridad de Validación y Autoridad de Certificación a entidades diferentes, con el fin de aislar la comprobación de la vigencia de un certificado electrónico de los datos de identidad del titular. Así, la Autoridad de Certificación (Dirección General de la Policía) no puede acceder a los datos de las transacciones que se realicen con los certificados que emite. Y las Autoridades de Validación no tienen acceso a la identidad de los titulares de los certificados electrónico que maneja.

2.2. Seguridad en el DNI electrónico

Uno de los principales usos del DNI-e es la realización de la firma electrónica. Para poder utilizar esta funcionalidad, es indispensable disponer de funciones de seguridad:

1. **Autenticación:** se dispone de distintos métodos de autenticación, mediante los cuales una entidad externa demuestra su identidad, o el conocimiento de algún dato secreto almacenado en la tarjeta. Entre los distintos tipos de autenticación podemos destacar: *autenticación de usuario (PIN)*, *autenticación de usuarios mediante datos biométricos*, *autenticación de aplicación* y *autenticación mutua*.
2. **Securización de mensajes:** se permite la posibilidad de establecer un canal seguro entre el terminal y la tarjeta que securice los mensajes transmitidos. 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 del canal.
3. **Desbloqueo y cambio de PIN:** se permite el cambio de PIN. Debido a la criticidad de esta operación, el cambio de PIN se ha de realizar siempre en condiciones de máxima confidencialidad y seguridad.
4. **Funcionalidad criptográfica:**
 - *Claves RSA:* genera y gestiona claves RSA. Se usa el algoritmo Miller-Rabin como test de primalidad.
 - *Hash:* realiza hash de datos con el algoritmo SHA1. Es posible realizar todo el proceso en la tarjeta o finalizar un hash calculado externamente.
 - *Firmas electrónicas:* puede realizar firmas electrónicas de distintos modos.
5. **Intercambio de claves:** esta operación es usada para compartir claves simétricas entre dos entidades. Es posible cifrar una clave *K_s* con la clave pública de un destinatario, la cual puede ser cargada en la memoria de la tarjeta protegida mediante una clave RSA. Y el destinatario puede descifrar la clave *K_s* usando la clave privada RSA correspondiente.

Sin embargo, el uso de las funciones de seguridad no determina que se puedan encontrar vulnerabilidades en el DNI-e, por ejemplo *en 2017 la Policía desactivó la firma digital del DNI ante un posible fallo de seguridad en el sistema de identificación online, que permitía hacer diversos trámites administrativos, mercantiles y privados. Debido a este problema un atacante podría calcular la porción privada de una clave vulnerable usando tan solo la parte pública. Eso daría lugar a que un atacante acabara pudiendo suplantar la personalidad de la víctima para descifrar datos sensibles, ocultar software malicioso en software firmado digitalmente o superar la protección basada en estos sistemas* (para más información, pincha [aquí](#)).

2.3. ¿Que ventajas nos ofrece el DNI electrónico?

Gracias al DNI electrónico, cualquier persona puede realizar múltiples gestiones online de forma segura con distintas personas y/o entidades, sin embargo, esas no son todas las ventajas que ofrece:

- **Respecto a las relaciones entre ciudadanos:** la firma electrónica del DNI-e 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. Además, proporciona el máximo grado de confidencialidad y seguridad en Internet, identifica a las partes que se conectan telemáticamente y permite el acceso seguro a servicios de Administración Electrónica desde dispositivos móviles.
- **Respecto a las relaciones con las Administraciones Públicas:** la Administración General del Estado es uno de los principales proveedores de servicios a 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 es necesario la presencia física para garantizar la identidad.
- **Respecto a las relaciones con las empresas:** las empresas deben desarrollar diferentes servicios basados en la identificación y firma electrónica, de forma que dinamicen la relación comercial con sus clientes. Por eso, desde el punto de vista empresarial y comercial, el DNI electrónico pasa a convertirse en una herramienta fundamental para las relaciones en el sector privado.

2.4. ¿Cómo utilizar el DNI electrónico?

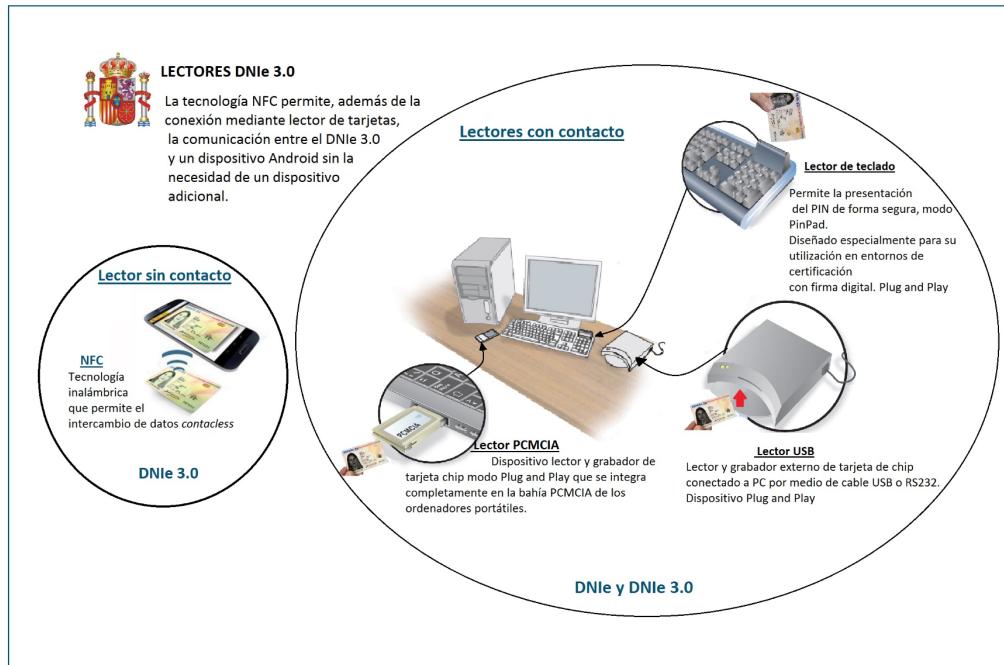


Figura 9: Utilización del DNI-e

Para hacer uso del certificado que incluye el DNI electrónico lo único que se necesita es el carnet de identidad, ya que en ese momento se proporciona un sobre con el PIN del DNI-e. Por el contrario, si se decide utilizar los certificados del DNI electrónico se

deberá adquirir un lector de tarjetas y renovar los certificados en el tiempo estipulado. Asimismo, para firmar con el DNI-e se necesita:

- Un ordenador personal.
- Un lector de tarjetas inteligentes.
- En cuanto a software, el DNI electrónico es compatible con los sistemas operativos actuales, así como con los distintos navegadores.

2.5. Diferencias entre DNI-e y DNI 3.0

Los cambios en la sociedad de hoy en día requieren de la constante actualización del DNI, esto ha supuesto la necesidad de mejorar y acercar a los ciudadanos su usabilidad. Por lo que la Dirección General de la Policía lanzó en 2015 el **DNI 3.0**. Sin embargo, tenemos que irnos hasta el año 2006 para presenciar que todos los Documentos Nacionales de Identidad que se expedían en España comienzan a ser documentos electrónicos.

Hoy en día, existen dos versiones: DNI-e y DNI 3.0, aunque el único documento que se expide actualmente es en el DNI 3.0. Hasta ahora hemos visto que el uso del DNI electrónico requiere de un dispositivo para la lectura de los datos del chip, así como la necesidad de la instalación de drivers necesarios para el funcionamiento del hardware, cosa que puede resultar complicada para un usuario normal.



(a) DNI-e

(b) DNI 3.0

Figura 10: Comparación del DNI-e con el DNI 3.0

La principal novedad del DNI 3.0 a su antecesor es la presencia de un chip con interfaz dual que permite la conexión mediante hardware, pero también de forma inalámbrica a través de la tecnología NFC (*Near Field Comunication*). No obstante tiene algunas ventajas como:

- Incorpora la tecnología de interfaz dual (NFC): gracias a un campo electromagnético entre el dispositivo y la tarjeta se puede intercambiar información. Lo que hace que no tenga la necesidad de utilizar un lector de tarjetas convencional.
- Para utilizarlo, solamente es necesario un dispositivo móvil con tecnología NFC y la app del servicio al que nos queremos conectar.

Por tanto, el ciudadano no tendrá que descargarse ningún certificado o driver, sino que la conexión se iniciará simplemente con acercar el DNI 3.0 a la antena NFC del dispositivo.

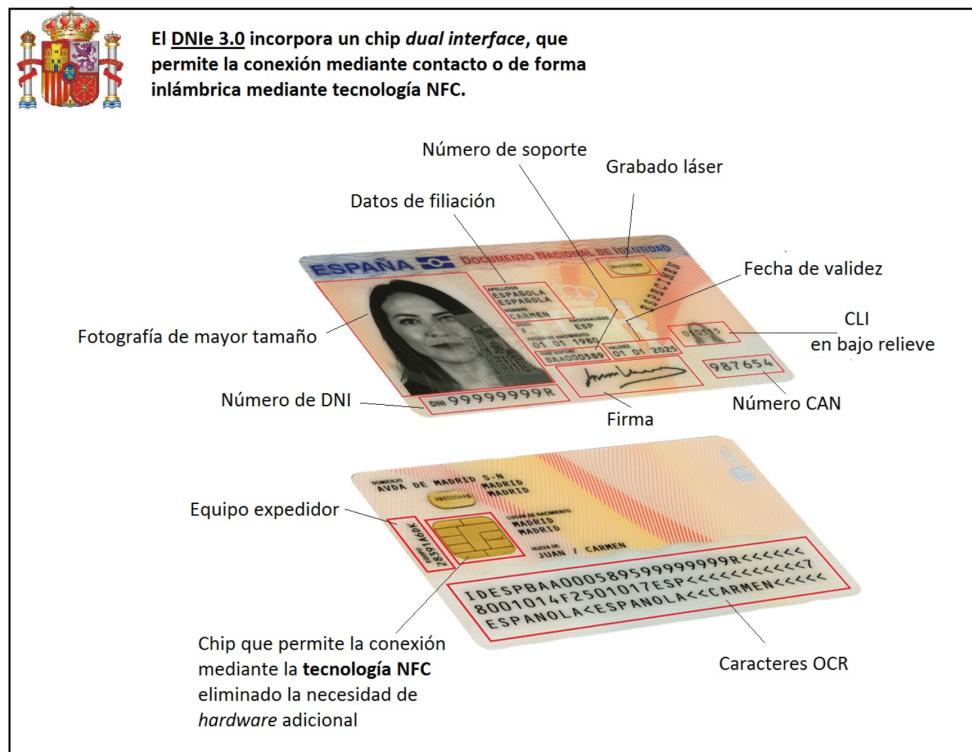


Figura 11: Descripción DNI 3.0



Figura 12: DNI-e y lector de tarjetas

3. Firma electrónica

El rápido avance tecnológico de la sociedad de hoy en día ha provocado un cambio en muchos hábitos de vida. Muchas acciones que antes se hacían de forma física o telefónicamente (declaración de la renta, compra, transacciones bancarias...), actualmente se pueden hacer sentados delante de un ordenador.

Como comentamos el inicio del trabajo, cuando firmamos un documento, estamos dando conformidad a lo que está escrito en ese documento. Por lo que una modificación sería detectable, pues dejaría huellas físicas. Además, al disponer la firma de unas características propias de la persona que firma, nadie podría suplantar esa firma. Podemos transpasar esta idea a los documentos digitales. En este caso, el añadido debería ser un conjunto de bits, y si éstos son los mismos para todos los documentos firmados por un usuario, cualquiera podría firmar un documento por él, cosa que no debería de producirse. Por tanto, la firma digital debe ser un añadido al documento que sólo pueda ser realizado por el firmante, pero que además deba variar con el mensaje, es decir, dependa del documento, en cuestión.

3.1. ¿Qué es la firma electrónica?

Una firma electrónica es un concepto legal.

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 reconocida tiene el mismo valor que la firma tradicional. Algunas características que debe satisfacer son:

- **Únicas:** sólo puede ser generada por el firmante.
- **Verificables:** debe ser fácilmente verificable, tanto por receptor como por jueces.
- **No repudiables:** el firmante no puede negar haber realizado la firma.
- **Viables:** la firma debe ser fácil de realizar.

3.2. ¿A qué nos referimos con firma digital?

Todas las firmas digitales son electrónicas, pero no todas las firmas electrónicas son digitales

En otro orden de ideas, debemos destacar que la **firma digital** no es sinónimo de firma electrónica, ya que ésta es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento, es decir, se refiere a la tecnología de cifrado/descifrado en la que se basan algunas firmas electrónicas. Por tanto, la firma electrónica pasa a ser un concepto más amplio que el de firma digital. Mientras que la firma digital hace referencia a una serie de métodos criptográficos, el concepto de firma electrónica es de naturaleza fundamentalmente legal, ya que confiere a la firma un marco normativo que le otorga validez jurídica.

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de

firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica. La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, no es posible, a partir del valor resumen, calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido.



Figura 13: Firma digital

Por tanto, la firma digital también es legal, pero no tiene naturaleza jurídica, en el sentido de que su objetivo no es dar fe de un acto de voluntad por parte del firmante, sino tan sólo encriptar los datos de un documento para conferirle mayor seguridad. La firma electrónica es una expresión genérica y mucho más amplia relativa a los datos electrónicos y la firma digital es la firma con criptografía basada en clave pública.



Figura 14: Firma digital

En resumen, la firma digital es una parte fundamental de la firma electrónica avanzada pero no de la firma electrónica simple (PIN ingresado en un cajero automático del banco o hacer clic en la casilla 'aceptar'). Ya que este tipo de firma electrónica no permite atribuir la firma a un firmante en concreto, por lo que no reúne las características de la firma digital.

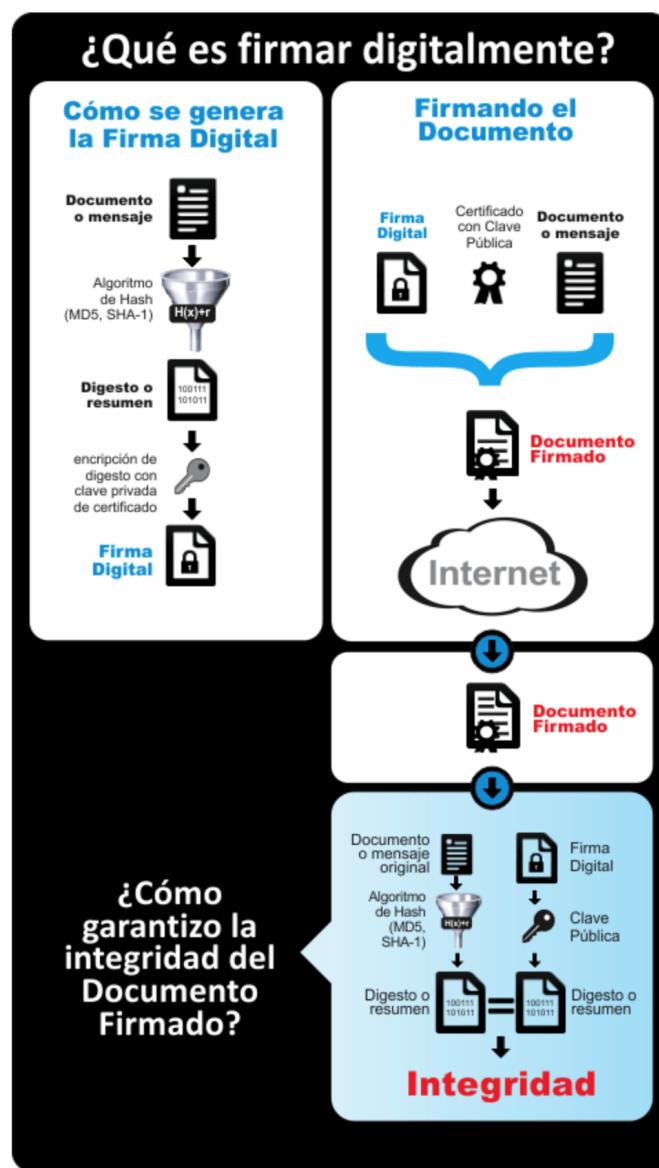


Figura 15: Funcionamiento de la firma digital

3.2.1. Ejemplo de implementación firma digital

En este punto se va **implementar un sistema de firma digital y verificación de la firma** con RSA. Para ello se deben de realizar tres tareas: **generación de claves**, **generación de firma** y **verificación de firma**.

El código completo se puede encontrar en mi Github:

https://github.com/Gecofer/MII_ASS_1819

1. Generación de claves

Para la generación de la clave, nos basamos en la función que implementa un **RSA**. El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de

bloques, que utiliza una clave pública, la cual se distribuye, y otra privada, la cual es guardada en secreto por su propietario. Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10^{100}) elegidos al azar para conformar la clave de descifrado². El algoritmo RSA funciona de la siguiente manera:

1. Para elegir la pareja de claves, lo primero que necesitamos es elegir dos primos grandes p y q , y calcular su producto $n = p \cdot q$.
2. Ahora se elige un entero e tal que $\text{mcd}(e, \phi(n)) = 1$. Recordemos que $\phi(n) = (p-1) \cdot (q-1)$. Ambos valores, (n, e) constituyen la clave pública del criptosistema. El número n se conoce como módulo del Criptosistema.
3. La clave privada es un entero d tal que $d \cdot e = 1 \pmod{\phi(n)}$.

Dichas claves de RSA, las guardaremos en un fichero. Por tanto, la función creada tiene como salida: e, n que será clave pública y d que será la clave privada.

```

import random
import fun_auxiliares as aux

# Método para generar una clave
# -----
def generacion_claves():

    # Por seguridad es conveniente elegir dos números de manera aleatoria
    p = random.randint(1, 1000000000000000)
    q = random.randint(1, 1000000000000000)

    # Si p no es primo, forzamos a que sea
    p = NextPrime(p)

    # Si q no es primo, forzamos a que sea
    q = NextPrime(q)

    # Realizamos su producto
    n = p*q

    # Calculamos phi
    phi = (p-1)*(q-1)

    e = 2
    # Elegimos un número 'e' que sea primo relativo con phi_n, sino aumentamos uno 'e'
    while(aux.alg_euclides_v2(phi,e)[0] != 1):
        e = e + 1

    # Para hallar la clave privada resolvemos la congruencia e·d = 1 (mod phi_n)
    # es decir, calculamos el inverso de 'e' en Z(phi_n)
    d = aux.alg_inverso(e,phi)

    # Abrimos los ficheros donde se guardarán las claves (debe tener permiso de escritura)
    try:
        f_pub = open("clave_publica", "w")
        f_priv = open("clave_privada", "w")
    except:
        print("Error abriendo los ficheros de las claves.")

    # Escribimos en un fichero la clave publica y privada, separando e y d de n con un espacio
    # Clave Pública
    f_pub.write(str(e)+" ")
    f_pub.write(str(n))
    # Clave Privada
    f_priv.write(str(d)+" ")
    f_priv.write(str(n))

    # Devolvemos las claves
    return e, n, d

# Para comprobar: e, n (clave publica) y d (clave privada)
e, n, d = generacion_claves()
print(e, n, d)

```

11 156715375538224370009061822677 85481113929939985489162164131

Figura 16: Función para generar las claves

²<https://seguinfo.wordpress.com/2007/09/14/%C2%BFque-es-rsa/>

2. Generación de firma

Para la **generación de la firma**, se le introducirá un mensaje a cifrar (fichero) y el fichero con la clave (privada), y deberá generar una firma, que se guardará en un fichero de texto. En este caso, el mensaje será *Hola*, y la clave privada la hemos obtenido en el apartado anterior. Puesto que lo que realmente se firma no es el mensaje, sino un resumen del mensaje, hay que generar un resumen de dicho mensaje. Para esto emplearemos la función **SHA1** (se pueden añadir otras funciones resumen). Dicha función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente.

```

import hashlib
import fun_auxiliares as aux

# Método para generar la firma
# -----
def generacion_firma(mensaje, clave_privada):

    # Abrimos el fichero de mensaje
    try:
        myfile = open(mensaje, encoding='utf-8')
    except:
        print("Error abriendo el fichero del mensaje.")

    # Lo guardamos en una variable
    m = myfile.read()
    m = m.encode("utf-8")

    # Calculamos un resumen del mensaje
    r = hashlib.sha1(m).hexdigest()

    # Como la salida de 'r' es en hexadecimal,
    # la convertimos a entero base 10 para poder operar con el resumen
    r = int("0x"+r, 0)

    # Leemos la clave del fichero
    try:
        f_priv = open("clave_privada")
    except:
        print("Error abriendo el fichero de la clave privada.")

    clave = f_priv.read().split(" ")
    d = int(clave[0])
    n = int(clave[1])

    # Generamos la firma (firma del resumen)
    f = aux.alg_potencia(r,d,n)

    try:
        f_firma = open("firma", "w")
    except:
        print("Error abriendo el fichero firma.")

    # Escribimos la firma en el archivo
    f_firma.write(str(f))

    # Devolvemos la firma
    return f

# Para comprobar

# Nombre del fichero de la clave privada
clave_privada = "clave_privada"

# Nombre del fichero del mensaje
mensaje = "mensaje"

firma = generacion_firma(mensaje, clave_privada)
print(firma)

```

153628067459055100918638374785

Figura 17: Función para generar la firma

Para la función SHA1, usaremos la librería de Python **hashlib**, que ya implementa esa función. Para generar una firma, solo nos bastaría hacer $fir(r) = r^d \pmod{n}$. Por tanto, el mensaje firmado sería el par $(r, fir(r))$.

- Entrada de la función:

1. *mensaje*: nombre del fichero del mensaje a firmar en string
2. *clave - privada*: nombre del fichero de la clave privada en string (contiene *d* y *n*)

■ **Salida** de la función:

1. *f*: firma del resumen del mensaje

3. Verificación de la firma

Para la **verificación de la firma**, se introduce el mensaje (fichero) que se ha firmado, un fichero con la firma (con el mismo formato que el generado en el apartado anterior) y un fichero con la clave (pública). Y deberá responder si la firma es o no válida. Para comprobar si la firma es válida, habría que hacer si $r = \text{fir}(r)^e \pmod{n}$.

```
import hashlib
import fun_auxiliares as aux

# Método para verificar la firma
# -----
def verificacion_firma(clave_publica, mensaje, firma):

    # Abrimos el fichero de mensaje
    try:
        myfile = open(mensaje, encoding='utf-8')
    except:
        print("Error abriendo el fichero del mensaje.")

    # Lo guardamos en una variable como string
    m = myfile.read()
    m = m.encode("utf-8")

    # Calculamos un resumen del mensaje
    r = hashlib.sha1(m).hexdigest()

    # Como la salida de 'r' es en hexadecimal,
    # la convertimos a entero base 10 para poder operar con el resumen
    r = int("0x"+r,0)

    # Leemos la clave del fichero
    try:
        f_pub = open("clave_publica")
    except:
        print("Error abriendo el fichero de la clave pública.")

    clave = f_pub.read().split(" ")
    e = int(clave[0])
    n = int(clave[1])

    # Leemos el fichero con la firma
    try:
        f_firma = open("firma")
    except:
        print("Error abriendo el fichero de la firma.")

    f = int(f_firma.read())

    # Verificamos la firma
    v = aux.alg_potencia(f,e,n)

    # Si la verificación coincide con la función resumen es válido
    if(v==r):
        return True # Firma válida
    else:
        return False # Firma no válida
```

Figura 18: Función para verificar la firma

■ **Entrada** de la función:

1. *clave - publica*: nombre del fichero de la clave pública en string (*e* y *n*)
2. *mensaje*: nombre del fichero del mensaje a verificar en string
3. *firma*: nombre del fichero de firma en string

■ **Salida** de la función:

1. *True*: si la firma es correcta
2. *False*: si la firma no es correcta

```
# Nombre del fichero de la clave privada
clave_privada = "clave_privada"

# Nombre del fichero de la clave pública
clave_publica = "clave_publica"

# Nombre del fichero del mensaje
mensaje = "mensaje"

# Nombre del fichero de la firma
firma = "firma"

# Hacemos la Firma RSA
generacion_claves()
generacion_firma(mensaje, clave_privada)
verificacion_firma(clave_publica, mensaje, firma)
```

True

Figura 19: Comprobación del sistema y verificación de la firma digital

Con esto acabamos de comprobar la verificación de la firma, para un mensaje *Hola*. Por tanto, si queremos comprobar que la verificación funciona, solo hace falta editar el fichero de firma y realizar de nuevo la verificación, con lo que obtendremos un valor *False*.

4. Conclusiones

Después de analizar los distintos tipos de certificados y ver sus ventajas e inconvenientes, se ha de destacar la flexibilidad de la que dota el certificado software emitido por la FMNT. Pero es decisión del usuario, elegir la opción que mejor se aadecue a sus necesidades. Sin embargo, actualmente ambos tipos de certificados se complementan, ya que prácticamente todas las webs que disponen de certificado digital mediante software, también tienen la posibilidad de usar el DNI electrónico. Además, la necesidad de evolución en el mundo tecnológico supuso dar el salto del DNI electrónico al DNI 3.0, el cuál permite una mayor usabilidad del mismo al permitir el acceso y autenticación con él a través de la tecnología NFC y no de la necesidad de usar un lector de tarjetas, lo que complicaba su uso mediante la instalación de drivers y adquisición del lector.

Por otro lado, cabe destacar que la funcionalidad del DNI electrónico, se basa fuertemente en la firma electrónica, la cual permite la identificación del firmante. Además, es importante señalar que esta firma tiene el mismo valor que la firma tradicional, cosa que con el certificado software no ocurre.

No obstante, las nuevas tecnologías del futuro evolucionarán hacia tecnologías más seguras y hacia la unificación de un único medio digital para la realización de dicha autenticación e identificación, pero aún queda mucho por recorrer.