



Certificados Digitales

DNI Electrónico

Certificados Digitales

DNI Electrónico

Trabajo para la asignatura de *Administración de Sistemas y Seguridad*



Gema Correa Fernández

✉ gecorrea@correo.ugr.es

 Gecofer

“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.”

– Certificado Digital

Contenido

1 Certificado digital

1.1 ¿Qué es el certificado digital?

1.2 ¿Qué son las claves digitales?

1.3 Formato de los certificados digitales

1.4 Tipos de certificados digitales

2 DNI electrónico

2.1 Componentes del DNI electrónico

2.2 Diferencias entre DNI-e y DNI 3.0

3 Firma electrónica

3.1 ¿Qué es la firma electrónica?

3.2 ¿A qué nos referimos con firma digital?

4 Conclusiones



Contenido

1 Certificado digital

1.1 ¿Qué es el certificado digital?

1.2 ¿Qué son las claves digitales?

1.3 Formato de los certificados digitales

1.4 Tipos de certificados digitales

2 DNI electrónico

2.1 Componentes del DNI electrónico

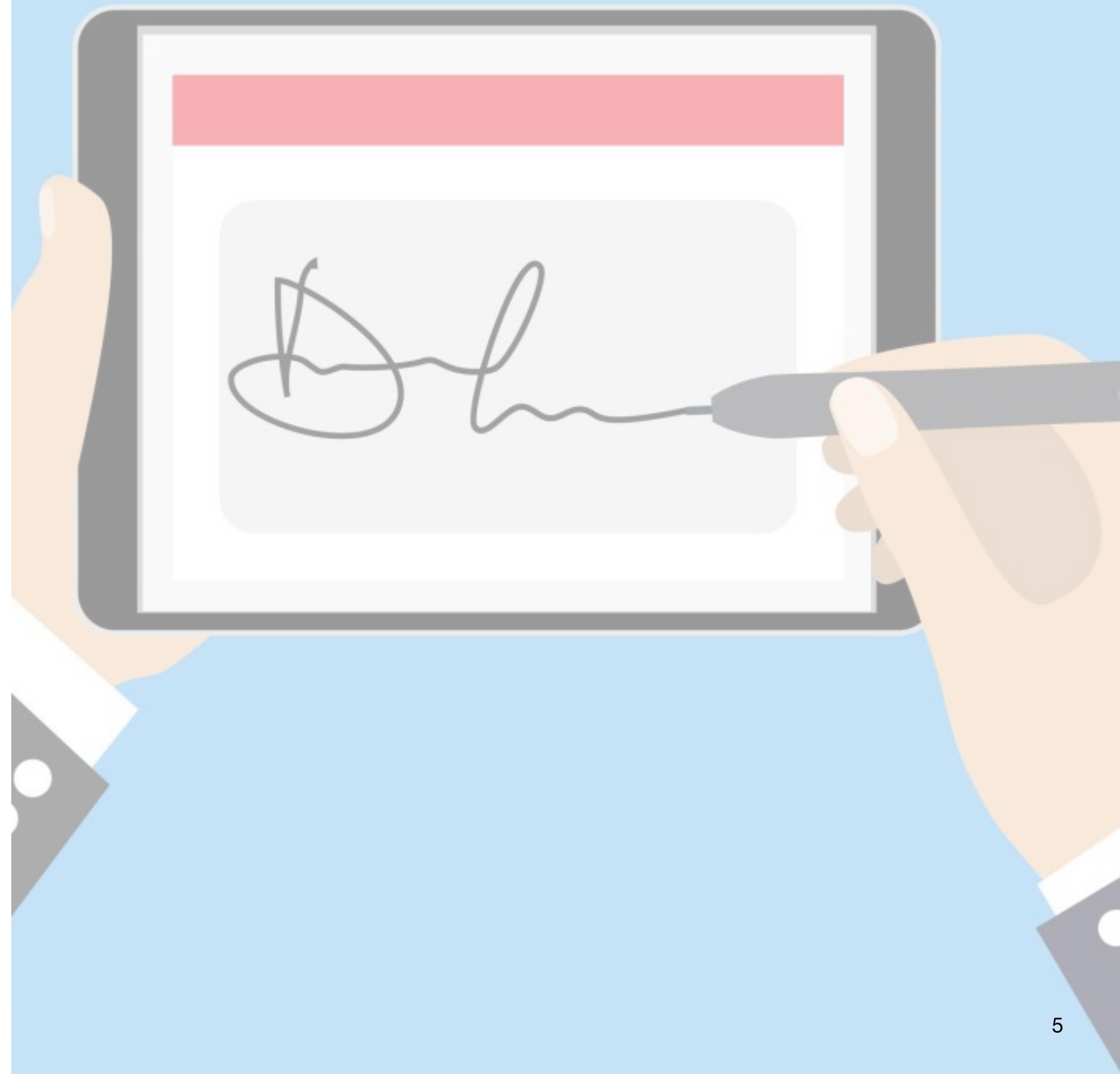
2.2 Diferencias entre DNI-e y DNI 3.0

3 Firma electrónica

3.1 ¿Qué es la firma electrónica?

3.2 ¿A qué nos referimos con firma digital?

4 Conclusiones



¿Qué es el Certificado Digital? (I)

- 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?*
- 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.
- Un **Certificado Digital** o **Certificado Electrónico** es un documento que identifica a una persona con un par de claves y va firmado digitalmente por quién lo emite.
- Es expedido por una **Autoridad de Certificación**.

¿Qué es el Certificado Digital? (II)

- Es el **único medio** que permite **garantizar técnica y legalmente la identidad de una persona en Internet**.
- Su objetivo es **validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta**, requisito para que las instituciones puedan ofrecer servicios seguros a través de la red.
- Todo certificado digital debe tener **información** relativa al **propietario** del certificado, **información** relativa al **emisor** del certificado, **claves del propietario** y **firma digital del certificado** por el emisor.

¿Qué son las Claves Digitales?

- Un Certificado Digital consta de una pareja de **claves criptográficas**: una **clave pública** y una **clave privada**, esenciales para la firma e identificación del firmante. **Lo que codifica una clave sólo lo puede 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.

Formato X.509

Ejemplo de un certificado X.509

Versión
Número de serie
Algoritmo de firma
Entidad emisora
Periodo de validez
Datos del sujeto
Clave pública del sujeto
ID único de la entidad emisora
ID único del sujeto
Extensiones
Firma digital de la entidad emisora

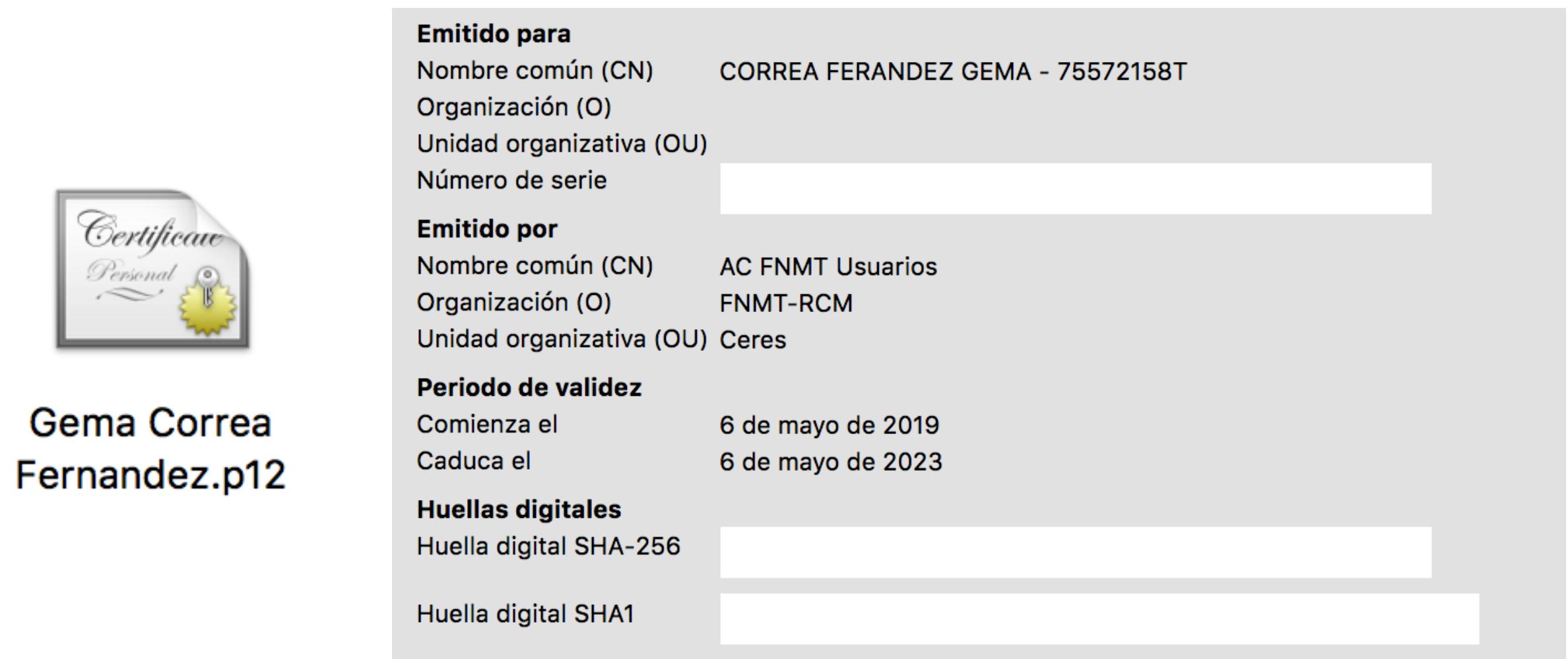
```
1 Certificate:  
2 Data:  
3 Version: 3 (0x2)  
4 Serial Number: 9 (0x9)  
5 Signature Algorithm: sha1WithRSAEncryption  
6 Issuer: C=US, ST=Florida, L=Tampa, O=Text CA,  
7 CN=bsd.jcs.local  
8 Validity  
9 Not Before: Mar 31 20:02:42 2003 GMT  
10 Not After : Mar 30 20:02:42 2004 GMT  
11 Subject: 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:a6:  
18 bd:c1:f0:10:b5:69:34:8c: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:af:85:1e: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:d5:6e:aa:a7:f0:2c: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:a0:1a: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:a9:c3:db:6b:a5:c3:ea:39:b7:9a:04:36:c9:  
32 de:d7:c2:ed:59:d7:bb:b9:4c:ec:35:a4:15: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:a8:59: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:a3:  
37 37:b6:ee:0f:44:07:1d:94:66:70:78:ef:31:d1:97:50:11:ec:  
38 25:c3
```

Tipos de Certificados Digitales (I)

- La obtención del Certificado Digital depende de si el **certificado está contenido en una tarjeta**, como el **DNI-e**, o de si el **certificado está en un fichero software**, emitido por la Fábrica Nacional de Moneda y Timbre.



DNI Electrónico



Certificado Digital emitido por la FNMT

Tipos de Certificados Digitales (II)

Características del Certificado Digital

La solicitud y descarga del certificado se realiza desde el navegador

Se instala en el navegador web en soporte fichero o soporte software

Cada proceso de solicitud depende de cada Autoridad de Certificación

Sólo funciona en los equipos en los que haya sido instalado, pero se puede exportar

Su duración suele ser de 36 meses

Características del DNI Electrónico

Al caducar el DNI, también extinguirán su validez los certificados

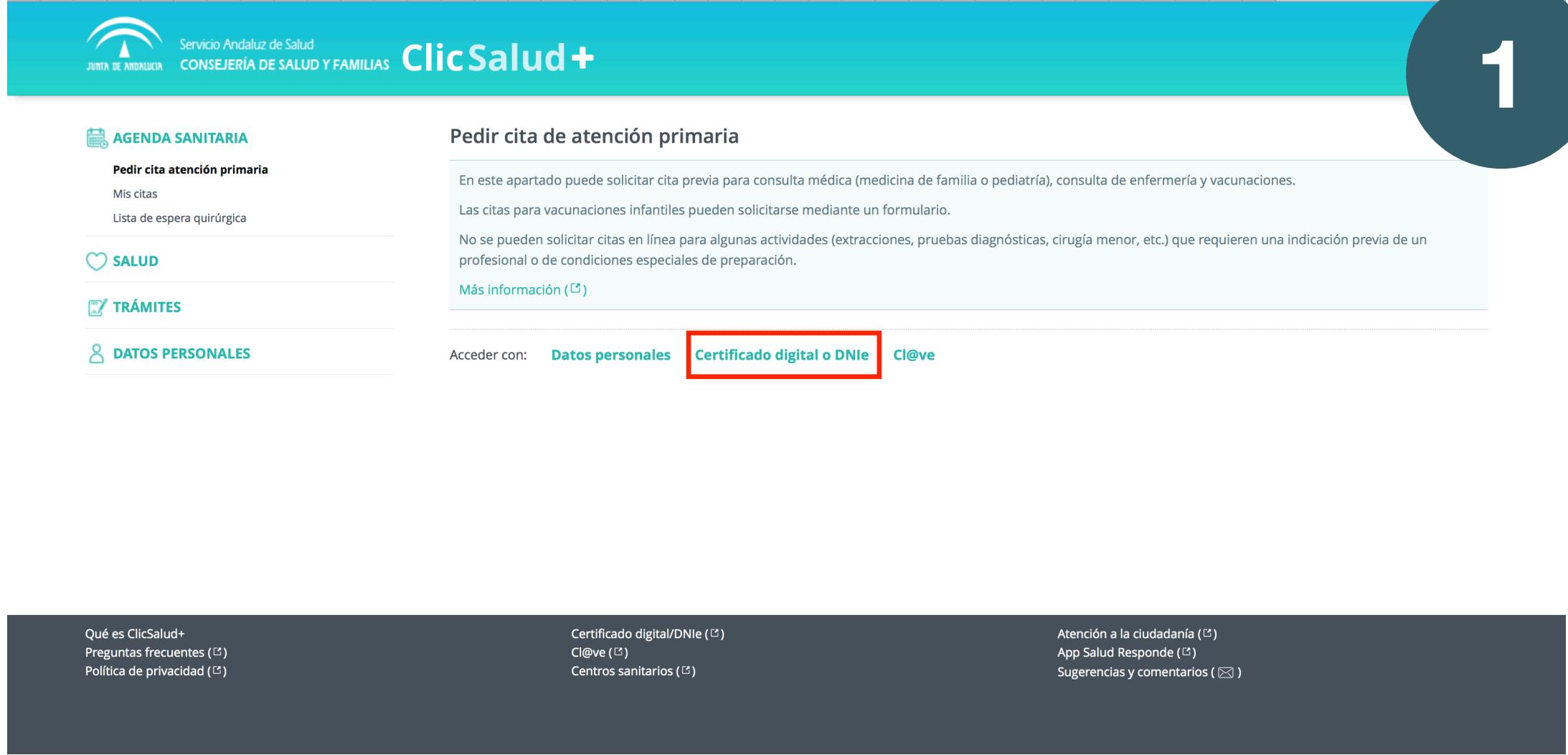
La firma electrónica con DNI-e es considerada como firma electrónica reconocida

Se necesita un lector de tarjetas en el caso de que se desee utilizar el DNI electrónico

Obtener estos certificados es gratis

Su duración suele ser de 30 meses

Funcionamiento del Certificado Digital



1

Servicio Andaluz de Salud
CONSEJERÍA DE SALUD Y FAMILIAS **ClicSalud+**

AGENDA SANITARIA
Pedir cita atención primaria
Mis citas
Lista de espera quirúrgica

SALUD

TRÁMITES

DATOS PERSONALES

Pedir cita de atención primaria

En este apartado puede solicitar cita previa para consulta médica (medicina de familia o pediatría), consulta de enfermería y vacunaciones.

Las citas para vacunaciones infantiles pueden solicitarse mediante un formulario.

No se pueden solicitar citas en línea para algunas actividades (extracciones, pruebas diagnósticas, cirugía menor, etc.) que requieren una indicación previa de un profesional o de condiciones especiales de preparación.

Más información (1)

Acceder con: **Datos personales** **Certificado digital o DNIe** Cl@ve

Qué es ClicSalud+
Preguntas frecuentes (1)
Política de privacidad (1)

Certificado digital/DNIe (1)
Cl@ve (1)
Centros sanitarios (1)

Atención a la ciudadanía (1)
App Salud Responde (1)
Sugerencias y comentarlos (1)



2

Servicio Andaluz de Salud
CONSEJERÍA DE SALUD Y FAMILIAS **ClicSalud+**

AGENDA SANITARIA
Pedir cita atención primaria
Mis citas
Lista de espera quirúrgica

SALUD

TRÁMITES

DATOS PERSONALES

Pedir cita de atención primaria

En este apartado puede solicitar cita previa para consulta médica (medicina de familia o pediatría), consulta de enfermería y vacunaciones.

Las citas para vacunaciones infantiles pueden solicitarse mediante un formulario.

No se pueden solicitar citas en línea para algunas actividades (extracciones, pruebas diagnósticas, cirugía menor, etc.) que requieren una indicación previa de un profesional o de condiciones especiales de preparación.

Más información (1)

Acceder con: **Datos personales** **Certificado digital o DNIe** Cl@ve

com.apple.WebKit.Networking desea firmar mediante la llave "privateKey" de tu llavero.
Para permitir esto, introduce la contraseña del llavero "Inicio de sesión".

Contraseña:

Permitir siempre Denegar Permitir

Qué es ClicSalud+
Preguntas frecuentes (1)
Política de privacidad (1)

Certificado digital/DNIe (1)
Cl@ve (1)
Centros sanitarios (1)

Atención a la ciudadanía (1)
App Salud Responde (1)
Sugerencias y comentarlos (1)



3

Servicio Andaluz de Salud
CONSEJERÍA DE SALUD Y FAMILIAS **ClicSalud+**

AGENDA SANITARIA
Pedir cita atención primaria
Mis citas
Lista de espera quirúrgica

SALUD

TRÁMITES

DATOS PERSONALES

Pedir cita de atención primaria (1)

1. Seleccionar tipo de cita

Medicina de familia Enfermería

Gema Correa Fernandez

Qué es ClicSalud+
Preguntas frecuentes (1)
Política de privacidad (1)

Certificado digital/DNIe (1)
Cl@ve (1)
Centros sanitarios (1)

Atención a la ciudadanía (1)
App Salud Responde (1)
Sugerencias y comentarlos (1)

Contenido

1 Certificado digital

1.1 ¿Qué es el certificado digital?

1.2 ¿Qué son las claves digitales?

1.3 Formato de los certificados digitales

1.4 Tipos de certificados digitales

2 DNI electrónico

2.1 Componentes del DNI electrónico

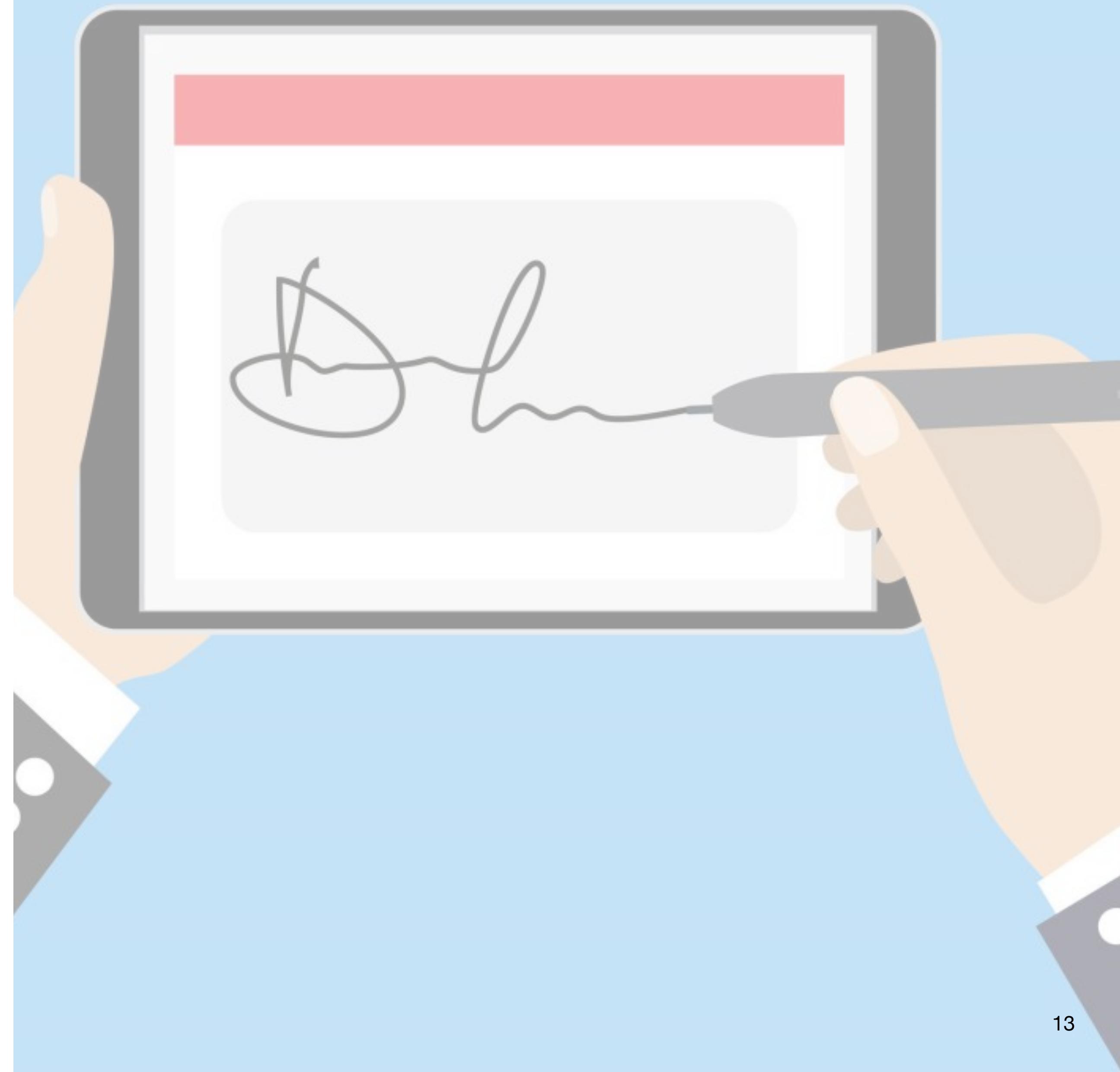
2.2 Diferencias entre DNI-e y DNI 3.0

3 Firma electrónica

3.1 ¿Qué es la firma electrónica?

3.2 ¿A qué nos referimos con firma digital?

4 Conclusiones

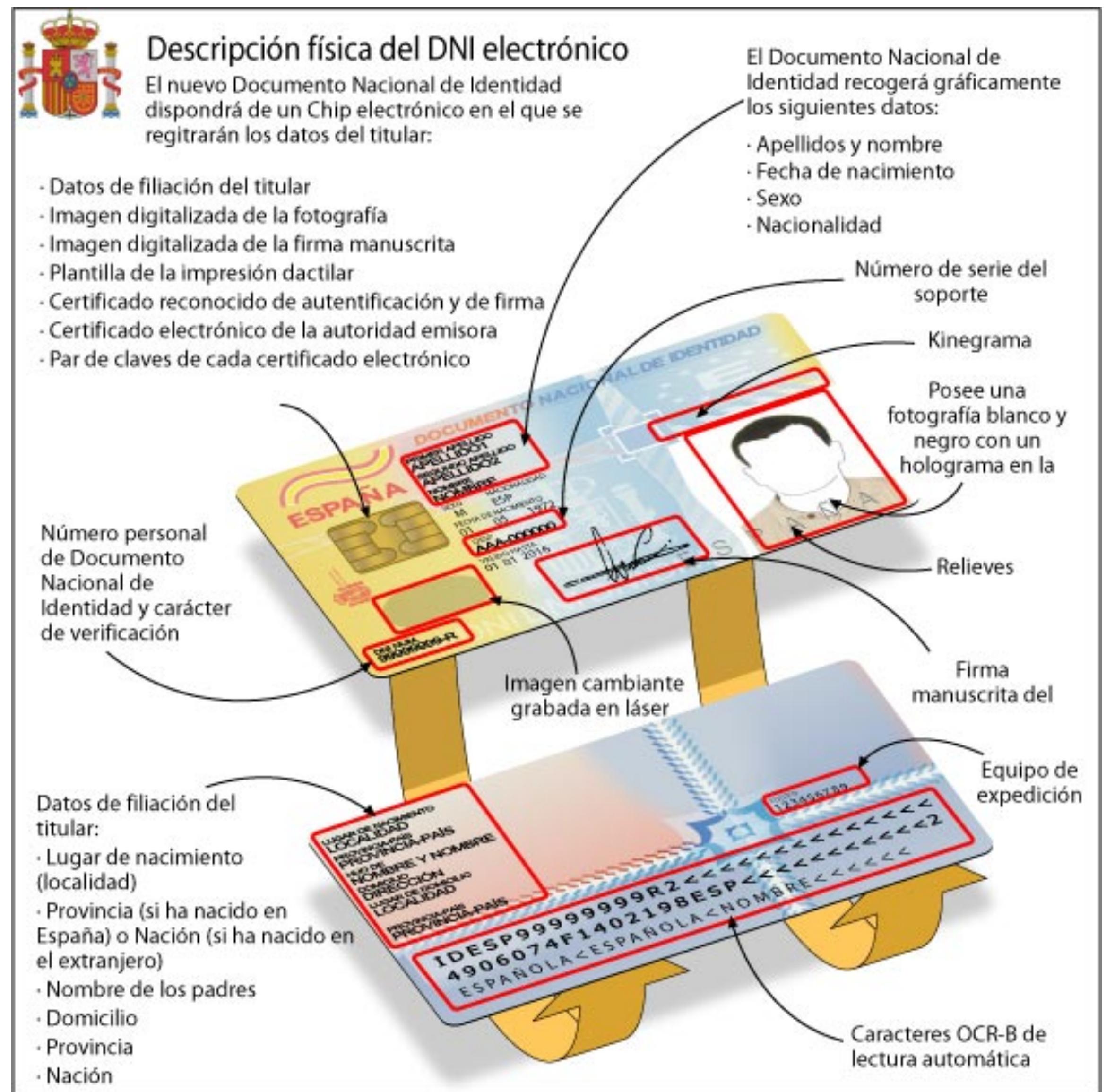


DNI Electrónico

- Documento emitido por la **Dirección General de la Policía** (Ministerio del Interior), sirve para:
 - **Confirmar la identidad** de una persona concreta
 - **Acreditar electrónicamente** y de forma inequívoca la identidad de la persona.
 - **Realizar firmas digitales en documentos electrónicos**, misma validez que la firma tradicional.
- Incorpora un 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.
 - **Certificado de Autenticación:** tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática.
 - **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.

Componentes DNI-e

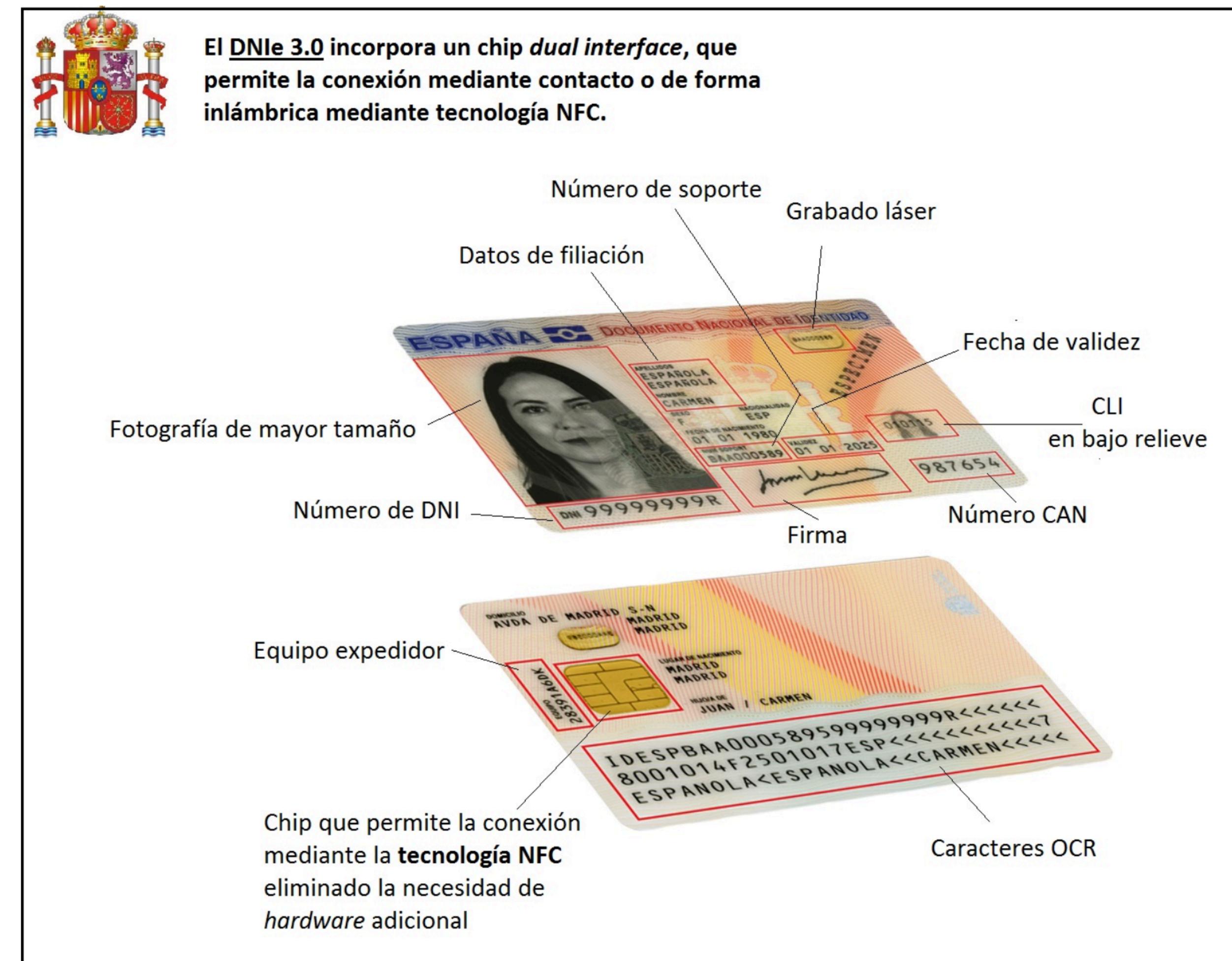
- **El chip criptográfico** contiene:
 - Datos de filiación del titular
 - Imagen digitalizada de la fotografía
 - Imagen digitalizada de la firma
 - Plantilla de impresión dactilar
 - Certificado de Autenticación y Firma
 - Certificado electrónico de la autoridad
 - Par de claves de cada certificado
- Contiene el SO DNle v1.1 con una capacidad de información de 32KB. Dicha información está **clasificada en zonas diferentes según su accesibilidad**. Se utiliza para firmar electrónicamente SHA-1 y usa claves RSA.



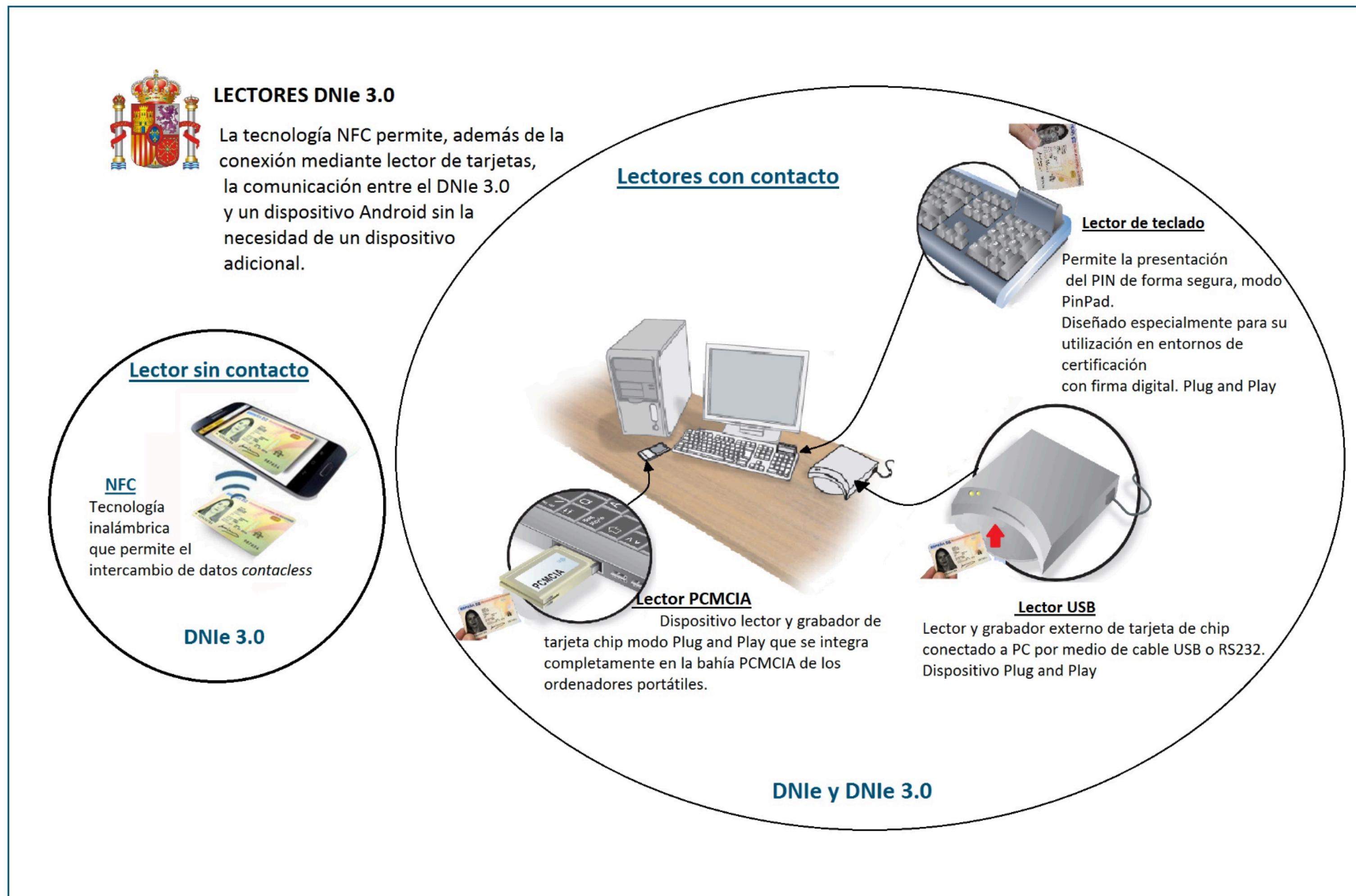
Descripción física del DNI-e

Diferencias DNI-e y DNI 3.0

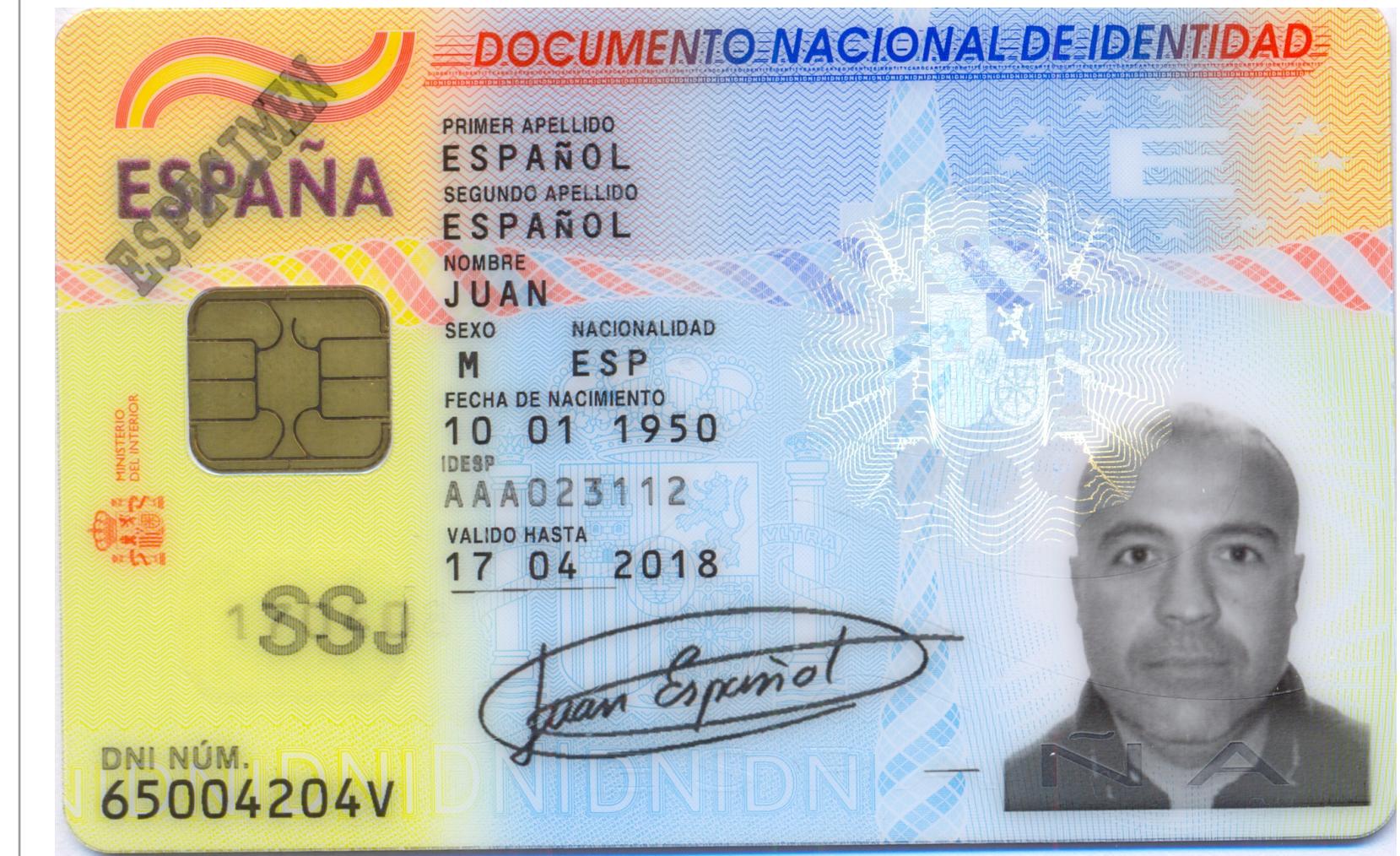
- La Dirección General de la Policía **lanzó en 2015 el DNI 3.0:**
 - Incorpora la **tecnología** de interfaz dual (**NFC**): gracias a un campo electromagnético entre el dispositivo y la tarjeta se puede intercambiar información. No hace falta utilizar un lector de tarjetas.
 - Solamente es necesario un dispositivo móvil con tecnología NFC y la app del servicio al que nos queremos conectar.
 - El ciudadano no tendrá que descargarse ningún certificado o *driver*, sino que la conexión se iniciará con acercar el DNI 3.0 a la antena NFC del dispositivo.



Descripción física del DNI 3.0



Utilización del DNI-e y DNI 3.0



DNI 3.0

Contenido

1 Certificado digital

1.1 ¿Qué es el certificado digital?

1.2 ¿Qué son las claves digitales?

1.3 Formato de los certificados digitales

1.4 Tipos de certificados digitales

2 DNI electrónico

2.1 Componentes del DNI electrónico

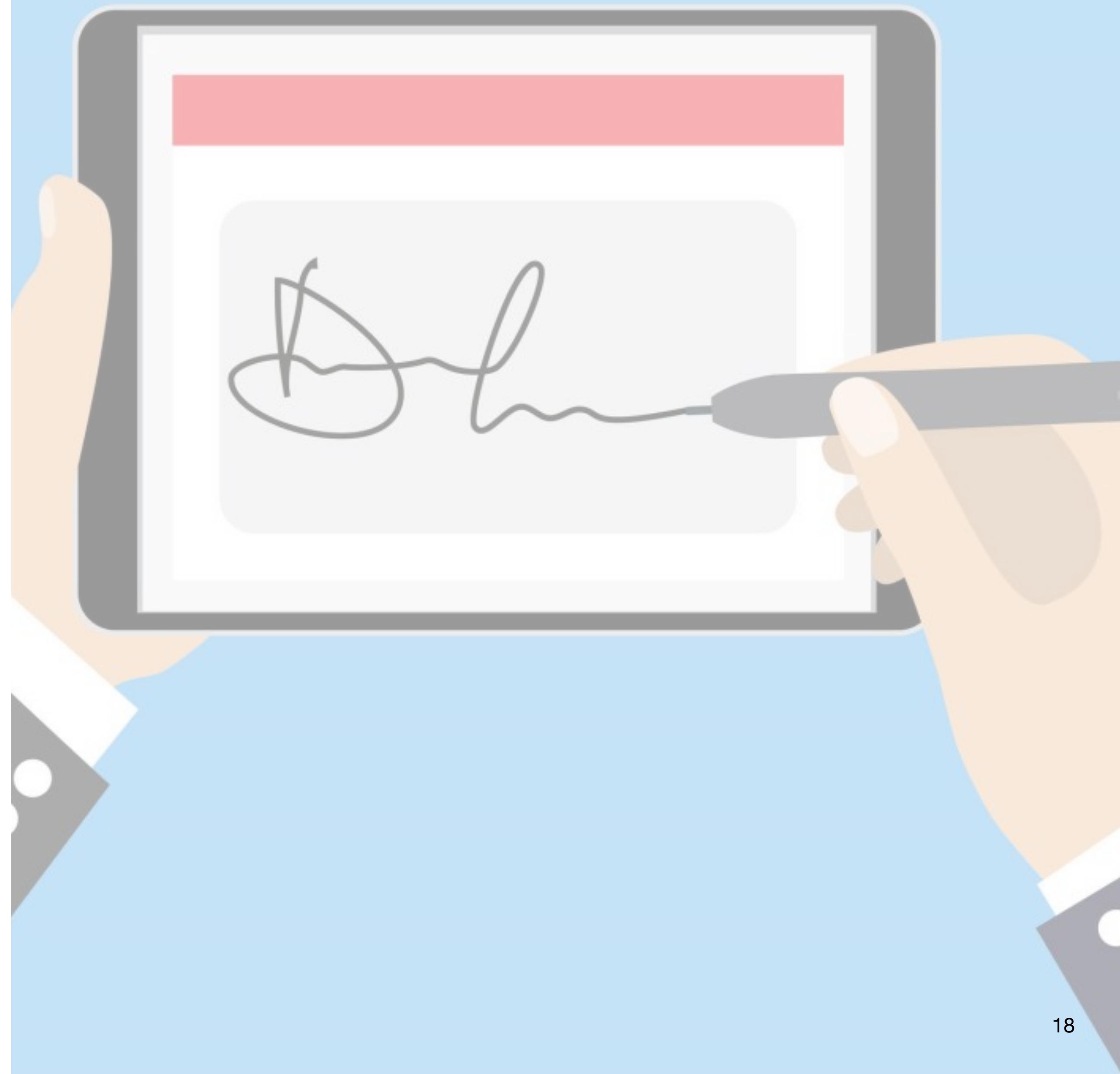
2.2 Diferencias entre DNI-e y DNI 3.0

3 Firma electrónica

3.1 ¿Qué es la firma electrónica?

3.2 ¿A qué nos referimos con firma digital?

4 Conclusiones



Firma Electrónica

- La **Firma Electrónica** es el conjunto de datos en forma electrónica, consignados junto a otros, que pueden ser utilizados como medio de identificación del firmante. La firma electrónica reconocida **tiene el mismo valor que la firma tradicional**. Algunas características satisface son:
 - **Únicas:** sólo puede ser generada por el firmante.
 - **Verificables:** debe ser fácilmente verifiable, tanto por receptor o jueces.
 - **No repudiables:** el firmante no puede negar haber realizado la firma.
 - **Viables:** la firma debe ser fácil de realizar.

Una firma electrónica es un concepto legal

¿A qué nos referimos con Firma Digital?

- La **Firma digital** no es sinónimo de Firma electrónica, ya que es un **método criptográfico** que asocia la identidad de una persona al mensaje/documento. Se refiere a la tecnología de cifrado/descifrado en la que se basan algunas Firmas Electrónicas.
- Mientras que la Firma Digital hace referencia a la encriptación de los datos de un documento para conferirle mayor seguridad, el concepto de Firma Electrónica es de naturaleza fundamentalmente legal, ya que confiere a la firma un marco normativo que le otorga validez jurídica.

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

¿Qué es firmar digitalmente?

Cómo se genera la Firma Digital



Firmando el Documento



¿Cómo garantizo la integridad del Documento Firmado?



Integridad

La Firma Digital

Clave Pública
(Compartida)



Emisor

"Hola"

Clave Privada
(Secreta)



Archivo

%\$&"#

Receptor

"Hola"

Firma Electrónica

Son unos datos electrónicos que acompañan la información (también en formato electrónico) e identifican al firmante.



Firma Digital

Permite que la firma electrónica (identificación y muestra de un acto de voluntad) pueda ser atribuida con seguridad a un firmante concreto.



Implementación de la Firma Digital

https://github.com/Gecofer/MII_ASS_1819

- Se ha **implementado un sistema de firma digital y verificación de la firma:**
 1. Para la **generación de la clave**, se usa el **sistema con clave pública RSA**, algoritmo asimétrico, que usa una clave pública que distribuye, y otra privada, que guarda en secreto.
 2. Para la **generación de la firma**, se introducirá el mensaje a cifrar y el fichero con la clave privada, y deberá generar una firma. Puesto lo que realmente se firma no es el mensaje, sino un **resumen del mensaje**, hay que generar un resumen de dicho mensaje (función **SHA1**).
 3. Para la **verificación de la firma**, se introduce el mensaje que se ha firmado, un fichero con la firma y un fichero con la clave pública.

```
# 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

Contenido

1 Certificado digital

1.1 ¿Qué es el certificado digital?

1.2 ¿Qué son las claves digitales?

1.3 Formato de los certificados digitales

1.4 Tipos de certificados digitales

2 DNI electrónico

2.1 Componentes del DNI electrónico

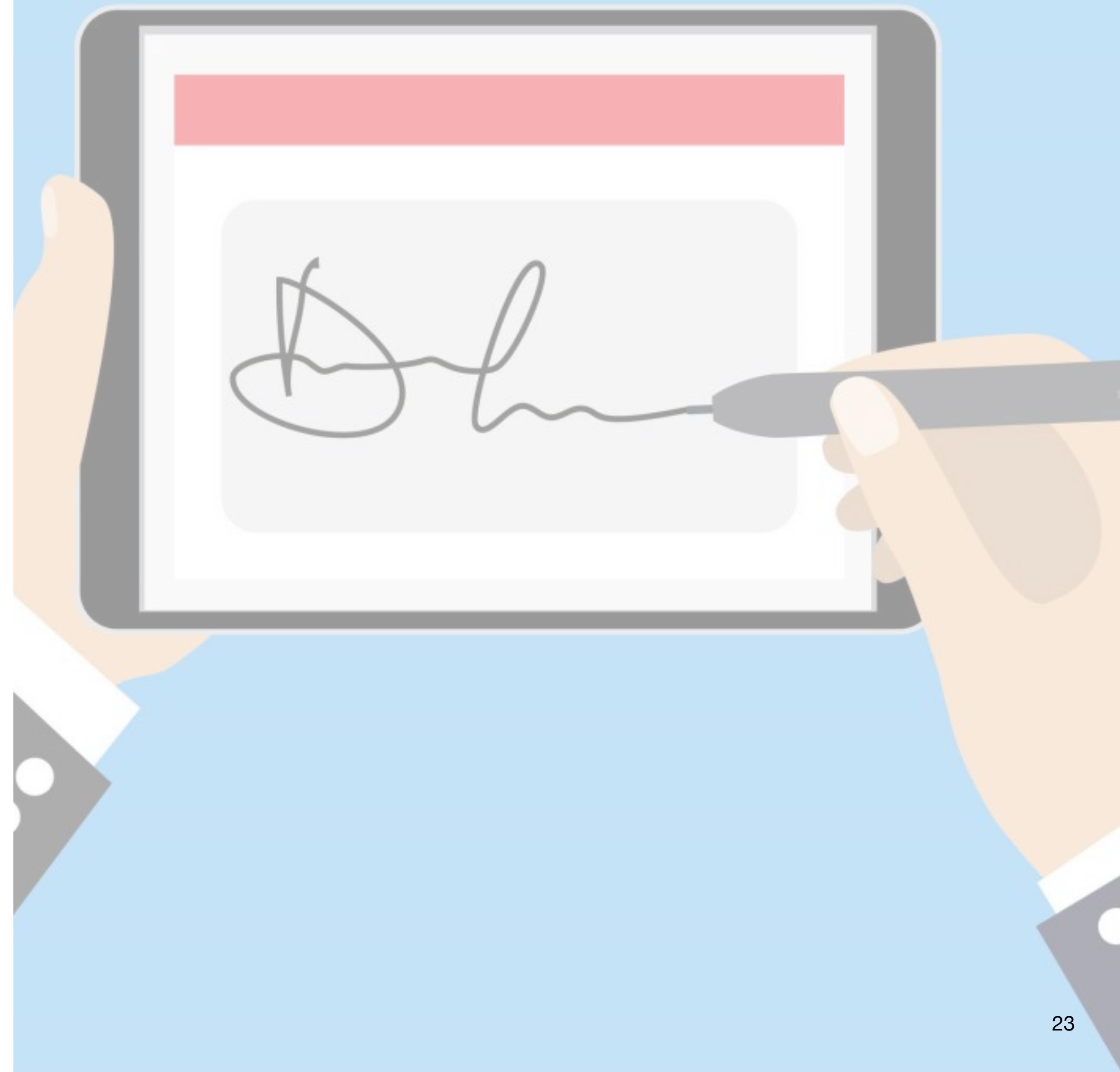
2.2 Diferencias entre DNI-e y DNI 3.0

3 Firma electrónica

3.1 ¿Qué es la firma electrónica?

3.2 ¿A qué nos referimos con firma digital?

4 Conclusiones



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 según a sus necesidades.
- Prácticamente todas las webs disponen de Certificado Digital y DNI Electrónico.
- La necesidad de evolución en el mundo tecnológico ha supuesto 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.
- 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.

Bibliografía más relevante

- [1] Jesús García Miranda. *Apuntes de Criptografía*. Curso 2016-2017
- [2] Cuerpo Nacional de Policía. *DNI Electrónico*. <https://www.dnielectronico.es/PortalDNle/>
- [3] Portal Administración Electrónica. *Los Certificados Electrónicos*
<https://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html>
- [4] Blog Junco TIC. *X509: Certificados digitales y codificaciones DER, CRT y CER*
<https://juncotic.com/x509-certificados-digitales-der-crt-cer/>
- [5] Xataka. *La seguridad del DNI electrónico, comprometida: a quién afecta, por qué y cómo solucionarlo*
<https://www.xataka.com/seguridad/la-seguridad-del-dni-electronico-comprometida-a-quien-afecta>
- [6] Admin fácil. *DNI electrónico vs Certificado digital: Usos y diferencias*
<https://www.adminfacil.es/dni-electronico-vs-certificado-digital/>



¡Gracias por su atención!
¿Preguntas?

Gema Correa Fernández

✉ gecorrea@correo.ugr.es

⌚ Gecofer