

# DNle

Documento nacional de identidad  
electrónico

# Introducción

- Documento que acredita la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular.
- Sociedad de la información: necesario introducir un instrumento que posibilite, la acreditación electrónica de la identidad de una persona y la firma digital de documentos electrónicos, otorgándoles validez jurídica equivalente a la que les proporciona la firma manuscrita.

- Se crea el **Documento Nacional de Identidad electrónico (DNle)**.
- Similar al tradicional, pero incorpora un pequeño circuito integrado, capaz de guardar información de forma segura y de procesarla internamente .
- Soporte tradicional (cartulina plastificada), fue cambiado por una tarjeta de material plástico, dotado de mayores medidas de seguridad.

# Usos

- Además del uso tradicional, permite acceder a servicios que amplían nuestras capacidades de actuar a distancia con las administraciones públicas, con las empresas y con otros ciudadanos.
- - Realizar compras firmadas a través de internet.
- - Hacer trámites con administraciones públicas a cualquier hora y sin colas.
- - Realizar transacciones seguras con entidades bancarias.
- - Identificarse electrónicamente para acceder a un edificio.

# ¿Que incorpora el chip del DNle?

- Los mismos datos que aparecen impresos en la tarjeta, filiación, fotografía, firma digitalizada y resumen criptográfico de la impresión dactilar, además de los certificados de autenticación y firma electrónica y un certificado de componente propio del DNle.

# ¿Cómo se distribuye la información en su interior?

- Tres zonas con diferentes niveles y condiciones de acceso:
  - - Zona pública
  - - Zona privada
  - - Zona de seguridad

- Zona pública: se puede acceder a ella sin restricciones. Contiene:
  - - Certificado CA intermedia emisora.
  - - Claves Diffie-Hellman.
  - - Certificado x509 de componente.

- Zona privada: solo puede acceder a ella el titular, mediante la clave personal de acceso o PIN. Contiene:
  - - Certificado de Firma (No Repudio).
  - - Certificado de Autenticación (Digital Signature).



- Zona de seguridad: solo puede acceder el titular, mediante los Puntos de Actualización del DNIe. Contiene:
  - - Datos de filiación del ciudadano (los mismos que están en el soporte físico).
  - - Imagen de la fotografía.
  - - Imagen de la firma manuscrita.

- Datos criptográficos: claves de ciudadano.  
Contiene:
  - - Clave RSA pública de autenticación (Digital Signature).
  - - Clave RSA pública de no repudio (ContentCommitment).
  - - Clave RSA privada de autenticación (Digital Signature).
  - - Clave RSA privada de firma (ContentCommitment).
  - - Patrón de impresión dactilar.
  - - Clave Pública de root CA para certificados card-verificables.
  - - Claves Diffie-Hellman.

- Datos de gestión:
  - - Traza de fabricación.
  - - Número de serie del soporte.
- El chip almacena los siguientes certificados electrónicos:
  - - Certificado de Componente
  - - Certificado de Autenticación
  - - Certificado de firma

# ¿Cómo se puede utilizar?

- Para realizar transacciones electrónicas, se necesita un lector de tarjetas inteligentes (con chip), con sus correspondientes drivers, conectado con un PC, la librería para hacer uso del DNle (CSP para S.O. Microsoft o PKCS#11) y tener conexión a internet. Se coloca el DNI en el lector, se introduce el PIN y se realiza la transacción.

# Bibliografía

- <http://www.dnielectronico.es/>
- <http://www.usatudni.es/dnie/>