**CARACTERÍSTICAS TÉCNICAS DNIe 3.0**

- Chip:
  - SLE78CLFx408AP de Infineon Technologies.
  - Características:
    - 400KB memoria Flash (código + personalización)
    - 8 KB memoria RAM
    - Dual Interface.
    - Criptolibrería RSA
    - CC EAL5+

- Algoritmos criptográficos soportados:
  - RSA
    - Longitud de claves de hasta 2048 bits en formato CRT y de hasta 1024 bits en formato normal.
    - Generación de claves RSA según el estándar PKCS#1.
  - Algoritmo de hash SHA-256 en la validación de certificados y en los comandos de autenticación.
  - Cifrado simétrico Triple DES y AES.

- Estándares internacionales que cumple:
  - ISO 7816 - Partes 1/2/3/4. Protocolo de transmisión T=0.
  - ISO 14443 - Partes 1/2/3/4. Protocolo de transmisión T=CL.
  - Estructura interna de ficheros según el estándar PKCS#15.
  - Autenticación de la información intercambiada entre las dos partes; incorporación de checksum criptográfico de tipo MAC según ANSI X9.19 y DES.
  - Protocolo de establecimiento de las claves de sesión basado en el esquema propuesto en ISO/IEC 9798 Parte 3.
  - Cálculo de claves de sesión se realiza según ANSI X9.63.
  - Establecimiento de canales seguros basados en EN 14890. (versión 2013).
  - Common Criteria EAL4+ aumentado con AVA_VAN.5.
  - Protection profiles for Secure signature creation device — Part 2: Device with key generation v2.0.1