RENIEC

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

DNI Electrónico

Identificación segura

Ing. Jaime Osorio Velasquez

Mayo 2015

DNI Electrónico

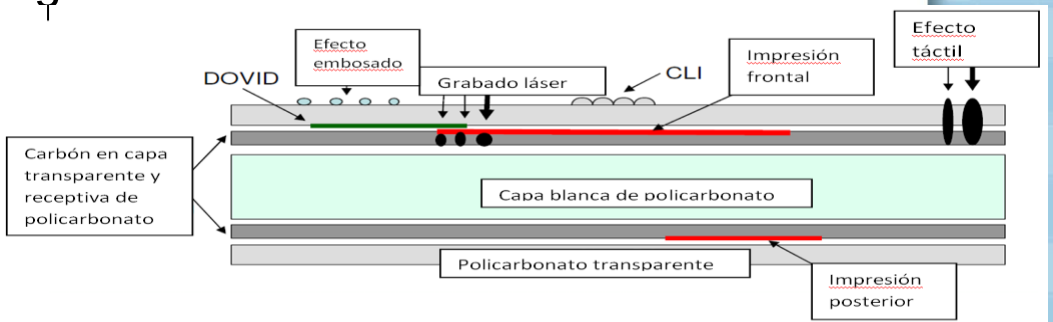
I. El DNI electrónico (DNIe)

- Documento Nacional de Identidad que consta de una tarjeta con un chip que incorpora cuatro aplicaciones de software.
- Se basa en las tecnologías de firma digital, de tarjeta inteligente (Smart Card) y biométrica, e incluye elementos de seguridad físicos y lógicos.
- Además de la identificación y autenticación presencial de las personas, según su uso tradicional, posibilita hacerlo por medios electrónicos y remotamente a través del Internet.

DNI Electrónico

II. Características generales del DNIe

- Chip con sistema operativo *Java Card.* Permite incorporación posterior de aplicaciones y contenidos.
- Tamaño ID1 – ISO 7810 (como una tarjeta de crédito).
- Chip con capacidad criptográfica para gestión de claves RSA y firma digital con certificados.
- Memoria EEPROM de 144Kb.
- Seguridad del chip según estándares *Common Criteria* nivel EAL4+ ó FIPS 140-2 level 3.
- El material de la tarjeta será policarbonato, el que permite la incorporación de elementos de seguridad física de última tecnología y su personalización mediante grabado láser.



III. Seguridad física del DNIe

- En el DNIe incorpora dispositivos de seguridad que cubran todos los tipos de amenazas, tanto en el nivel de inspección 1 como en el nivel de inspección 2.
- Además se incorporará un dispositivo bajo el nivel de inspección 3.

DNI Electrónico

III. Seguridad física del DNIe

Detalles de Seguridad

Microtexto con error deliberado

Fondo numismático

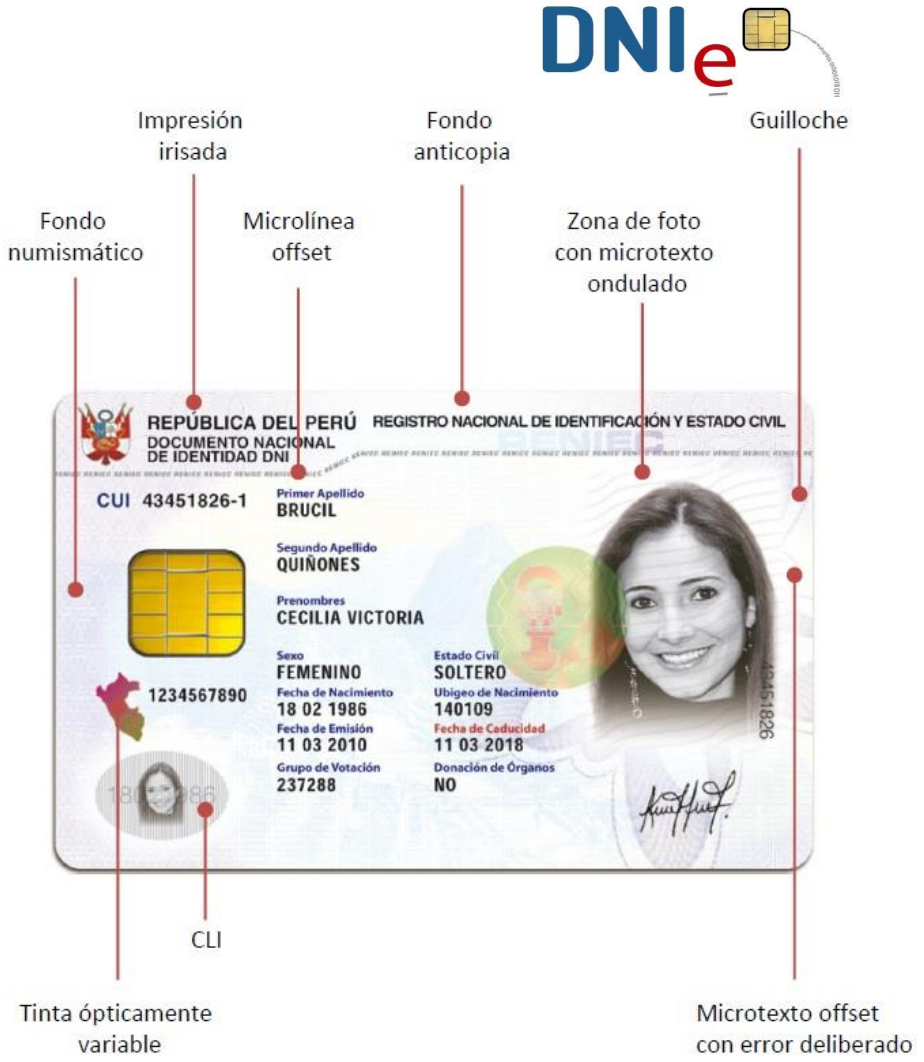
Tinta ópticamente variable
Vista de frente

Tinta ópticamente variable
Vista inclinada

Efecto de color a 0°

Efecto de color a 90°

CLI



IV. Niveles de inspección y tipos de amenazas para el DNIe

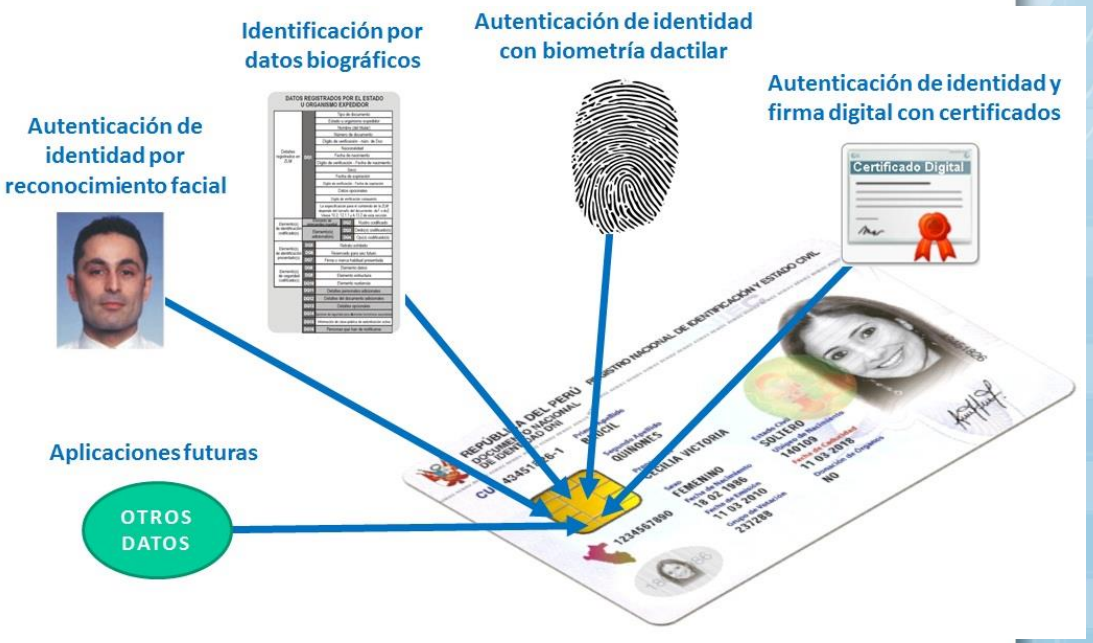
- Nivel de inspección 1. Referido a elementos de seguridad de conocimiento público cuya inspección no requerirá el uso de instrumentos.
- Nivel de inspección 2. Referido a elementos de seguridad de conocimiento público cuya inspección sí requerirá el uso de instrumentos (luz UV, lupa, escáner, filtros,...).
- Nivel de inspección 3. Referido a elementos sólo conocidos por el RENIEC y por los organismos de seguridad. Su inspección puede requerir o no del uso de herramientas o instrumentos.

- Amenaza de seguridad tipo 1: Falsificación o imitación.
- Amenaza de seguridad tipo 2: Alteración de datos en un DNI genuino.
- Amenaza de seguridad tipo 3: Sustitución de la fotografía.
- Amenaza de seguridad tipo 4. Canibalización o composición con partes de otros DNI genuinos.

DNI Electrónico

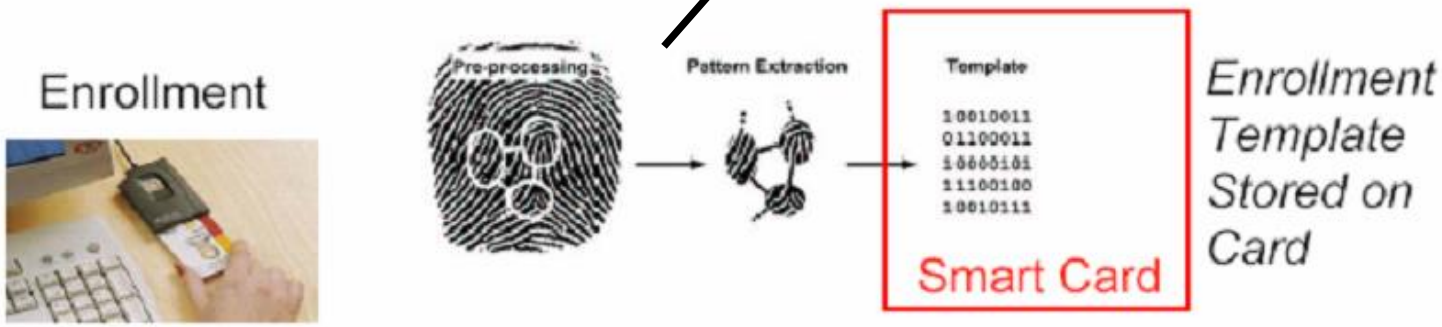
V. Aplicaciones del DNIe

1. **PKI:** Firma digital y autenticación
2. **MoC:** Match on Card
3. **Aplication ID - ICAO:** Documento de viaje
4. **ED:** Estructuras de datos (VE, SALUD, PS)



VI. Aplicación biométrica – MoC – Match on Card

El chip contiene las plantillas de las huellas dactilares (índice derecho e izquierdo), lo que posibilitará su comparación con las del portador, la aplicación Match on Card se encarga de realizar dicha comparación y de enviar el resultado positivo o negativo.



VII. Proceso de autenticación con la aplicación MOC

1. Para entornos presenciales.
2. Dentro del chip se encuentra grabada la plantilla de las huellas.
3. Un lector de tarjeta (Smart Card Reader) y un lector de huella deben estar disponibles en el computador.
4. Desde el computador se inicia la solicitud de verificación.
5. La imagen de la huella capturada es enviada a la tarjeta para su comparación con la plantilla almacenada.
6. Si la huella almacenada es la misma que la capturada, la tarjeta responde positivamente.

VIII. Elementos de Uso del Smart Card Reader

- Soporte tarjetas ISO 7816. Debe poder leer y escribir a tarjeta Smart Card compatibles con ISO 7816 1, 2, 3, 4
- Soporte PC/SC.
- Compatibilidad con Sistemas Operativos Windows XP, Windows 7 (32 y 64 bits) y superior, Linux Kernel 2.6 como mínimo.
- Microsoft® XP, Vista, Win7 mínimo.
- Comunicación a la PC por cable USB

IX. DNIe: Elementos de Uso: Lector de huella dactilar

- **Generación plantillas biométricas en formato estándar ISO/IEC 19794-2 COMPACT CARD.**
- Sensor óptico (CCD o CMOS).
- Resolución: 500 dpi.
- Área de captura mínima (a 500 dpi): 256 píxeles (ancho) x 360 píxeles (alto).
- Generación de imágenes en Escala de Grises de 256 tonos (8 bits).
- Conexión a PC por cable USB.
- Compatibilidad con Windows XP y Windows 7 como mínimo.
- De preferencia certificado por el FBI como dispositivo PIV SINGLE FINGER CAPTURE DEVICES y deberá estar listado en la siguiente direccion: http://www.fbi.gov/hq/cjisd/iafis/cert.htm, categoría “PIV SINGLE FINGER CAPTURE DEVICES” o http://www.fips201.com/category/view/11.

X. Comandos APDU

El **Application Protocol Data Unit** (**APDU**) por sus siglas en inglés o Unidad de Aplicación de Datos de Protocolo, es la unidad de comunicación entre un lector de tarjetas inteligentes y una tarjeta inteligente. La estructura de un APDU está definida en los estándares ISO/IEC 7816.

XI. Comandos APDU - Estructura

Un comando APDU tiene la siguiente estructura:

Dónde:

CLA : Clase de instrucción

INS : Instrucción propiamente dicha

P1y P2 : Parámetros de entrada

Lc : Longitud de la data

Data : Campo de datos

Le : Longitud esperada para la respuesta

Cada comando APDU siempre tiene una respuesta, la respuesta tiene la siguiente estructura:

XI.1. Comandos APDU – Estructura

Cada comando APDU siempre tiene una respuesta, la respuesta tiene la siguiente estructura:

Dónde:

Data : Datos de respuesta (opcional)

SW : (Status Word) Estado de ejecución del comando de envío

Muchas gracias