DOCUMENTO TÉCNICO

CÓDIGO:	VERSIÓN:	PÁGINAS:
DNIE-02-SGCD-GCRD-RENIEC	1.0	47
	FECHA: 30/09/2015	

GERENCIA:
CERTIFICACIÓN Y REGISTRO DIGITAL

SUB GERENCIA:
CERTIFICACIÓN DIGITAL

ACTIVIDAD MACRO:
DNI ELECTRÓNICO

Guía de referencia técnica del DNI electrónico

INTRODUCCIÓN

El DNI electrónico (DNIe) se viene desplegando de manera gradual y progresiva desde el 16 de julio del año 2013 en que se produjo su lanzamiento por parte del RENIEC. Las condiciones económicas favorables de los últimos años en nuestro país y los avances en las tecnologías de la información vienen propiciando la implementación por las entidades públicas de soluciones de gobierno electrónico. Por su parte, las imposiciones de la competitividad dentro de un mundo globalizado llevan también a que las empresas busquen la mejora de sus procesos y la automatización de los mismos. Además de ello, el ciudadano de a pié vive inmerso cada vez más dentro de entornos electrónicos, en particular en Internet, lo que le origina la necesidad de poder interactuar plena y eficazmente en este tipo de medios.

En este contexto, se desarrolla la *Guía de referencia técnica del DNI electrónico.* La guía presenta el nuevo documento de identidad señalando sus características técnicas tanto físicas como electrónicas, así como sus principales usos.

Este documento está dividido en dos partes. En la primera parte, se presentan sus características. En lo referido al aspecto físico, se describe el soporte de policarbonato de la tarjeta del DNIe con las características que le son inherentes, así como los diversos mecanismos de seguridad incrustados en él y provenientes de la pre-personalización, al igual que aquellos que resultan del proceso de personalización. El conocimiento de estas características contribuirá a la correcta validación del documento en entornos presenciales. A continuación se desarrolla lo correspondiente al perfil electrónico del DNIe, que trata lo referido al chip de contactos como microprocesador con capacidades criptográficas, además de lo relacionado con su sistema operativo JavaCard®, a las aplicaciones de software y a las estructuras de datos disponibles. Se refieren también las certificaciones de seguridad con que cuenta. Se espera que la difusión de esta información sirva para potenciar su utilización bajo las más diversas aplicaciones.

La segunda parte, está dirigida a los desarrolladores de aplicaciones de software que requieran integrar las capacidades del DNIe, mediante alguna de sus funcionalidades de autenticación de la identidad y/o firma digital. Si bien el middleware o drivers provistos por los fabricantes, así como los que se incluyen por defecto en los sistemas operativos, permiten que los ciudadanos puedan usar su DNIe en operaciones de gobierno y comercio electrónico básicas utilizando una PC (computadora personal), éste no necesariamente es el caso de uso más común en la actualidad. Debido al avance de la tecnología, hoy en día los ciudadanos están expuestos a diversos

dispositivos tales como tablets, smartphones, cajeros electrónicos, dispositivos POS (Point Of Sale), entre otros. Por tal motivo, a través del presente documento se pone a disposición de los fabricantes y los proveedores de hardware/software los comandos *APDU (Application Protocol Data Unit),* de manera que sean éstos quienes implementen aplicaciones específicas bajo dichas plataformas.

BASE LEGAL

La Ley Orgánica del Registro Nacional de Identificación y Estado Civil, RENIEC, Ley 26497, dada en Junio de 1995, define como una de sus funciones "Emitir el documento único que acredita la identidad de las personas, así como sus duplicados". Define además, en su Título V, las atribuciones y contenido del Documento Nacional de Identidad, DNI. En particular, su artículo 29° establece: "El Documento Nacional de Identidad (DNI) será impreso y procesado con materiales y técnicas que le otorguen condiciones de máxima seguridad, inalterabilidad, calidad e intransferibilidad de sus datos, sin perjuicio de una mayor eficacia y agilidad en su expedición".

Posteriormente, mediante Decreto Supremo N° 052-2008-PCM, se aprobó el Reglamento de la Ley de Firmas y Certificados Digitales N° 27269, de Julio del 2008. En su artículo 45 se define al Documento Nacional Electrónico DNIe, como una clase de DNI emitido por el RENIEC, que "acredita presencial y electrónicamente la identidad personal de su titular, permitiendo la firma digital de documentos electrónicos y el ejercicio del voto electrónico presencial y no presencial".

La definición del DNIe incluida en el referido Decreto Supremo del 2008 apunta a instrumentalizar la acreditación de identidad del ciudadano en entornos electrónicos. En ese contexto amplio de funciones, abarca también a las que dan sustento a la realización de la firma digital y al voto electrónico como razón de ser del documento DNIe, a las que considera factibles de implementarse. Conviene precisar el alcance de las enunciadas propiedades que dan origen al DNIe en el entorno actual de la tecnología de tarjetas inteligentes. Ellas, en principio, deben considerarse como adicionales a las propiedades de la tarjeta DNI convencional definidas por la Ley 26497.

PARTE I

ESPECIFICACIONES TÉCNICAS DEL DNI ELECTRÓNICO

1. DESCRIPCIÓN GENERAL DEL DNI ELECTRÓNICO

El Documento Nacional de Identidad electrónico (DNIe), es una tarjeta de material policarbonato, que tiene incrustado un módulo controlador electrónico "chip". Su diseño como dispositivo electrónico se enmarca en la tecnología de tarjetas inteligentes "smart card", las cuales son usadas a nivel mundial como tarjetas de identidad, tarjetas bancarias, o tarjetas de pago de tarifas. Para efectos de validar electrónicamente la información almacenada en su memoria, el DNIe dispone de recursos de hardware y software mediante los cuales ejecuta procedimientos criptográficos usando certificados digitales emitidos a nombre del ciudadano titular que lleva almacenados, incluyendo la realización de la firma digital. En base a procedimientos estándar, mediante el uso de dichos certificados digitales se hace posible también la validación de la identidad ante un servicio informático al cual se haya accedido desde el computador donde a través de un dispositivo lector se tiene conectado el documento de identidad.

También el DNIe ejecuta procedimientos de cotejo de información basados en algoritmos biométricos para validar la huella dactilar del ciudadano titular y en consecuencia su identidad.

Físicamente, la tarjeta DNIe conjuga varios aspectos de diseño que le confieren alta seguridad contra alteraciones o falsificaciones que pudieran afectar su reconocimiento y provocar fraude por impostores del usuario titular. Algunos de esos aspectos están asociados a la impresión gráfica, o al grabado de datos, o a la incorporación de dispositivos ópticos de seguridad.

Lógicamente, el chip incorporado en el DNIe, está fabricado para mantener inaccesibles ciertos sectores de memoria donde se almacenan códigos identificatorios del ciudadano, como son sus claves para operaciones criptográficas o sus plantillas biométricas de huellas dactilares, las cuales sólo son usadas internamente. Asimismo, el almacenamiento o lectura de otros datos en la memoria, es solo realizable mediante el uso de claves únicamente conocidas por el ente emisor, RENIEC, o por entidades previamente autorizadas, a través de la ejecución de las aplicaciones cargadas en el chip. Finalmente, existen también datos a los que se puede acceder de manera libre.

2. LA TARJETA

2.1 Soporte de policarbonato

El Documento Nacional de Identidad Electrónico es una tarjeta constituida por cinco láminas de material policarbonato, las cuales han sido fusionadas a altas temperatura y presión. Su consistencia es unitaria, firme y dura, pero que admite flexión, con resistencia al calor y a los rayos ultravioleta. Incrustado en el soporte de policarbonato, va el microprocesador o "chip". El conjunto de funcionalidades físicas y electrónicas de la tarjeta está diseñado para soportar su uso por el ciudadano durante sus 8 años de vida.

- Una capa de policarbonato transparente sirve de recubrimiento a la tarjeta por el anverso. Lleva por debajo de su superficie el dispositivo óptico de imagen variable por difracción, DOVID, estampado en caliente. En su superficie externa, sobre esta primera capa va impresa la estructura o patrón difractivo de soporte de las imágenes cambiantes CLI; y sobre ella también, el grabado láser produce en relieve los caracteres de la fecha de nacimiento, con efecto táctil, en la personalización.
- Una capa de policarbonato transparente, ubicada adyacente al recubrimiento del anverso. Ésta ha sido modificada químicamente para soportar el grabado láser (carbonizado) de alta resolución para los datos de personalización, incluidas fotografías, que se muestran en el anverso de la tarjeta. El haz láser atraviesa para ello la capa transparente superficial.
- Dos capas de policarbonato opaco, color blanco, inactivo a la reflexión de luz ultravioleta, constituyen el núcleo central de la tarjeta. Cada una de ellas sirve de soporte a la impresión según el diagramado y diseño gráfico del fondo de la tarjeta mediante técnicas de serigrafía y offset, correspondiendo tanto al anverso como al reverso. En la del anverso va depositado el elemento de tinta ópticamente variable OVI.
- Una capa de policarbonato transparente modificado químicamente para soportar la personalización gráfica de alta resolución del grabado láser, correspondiente al reverso del DNIe.

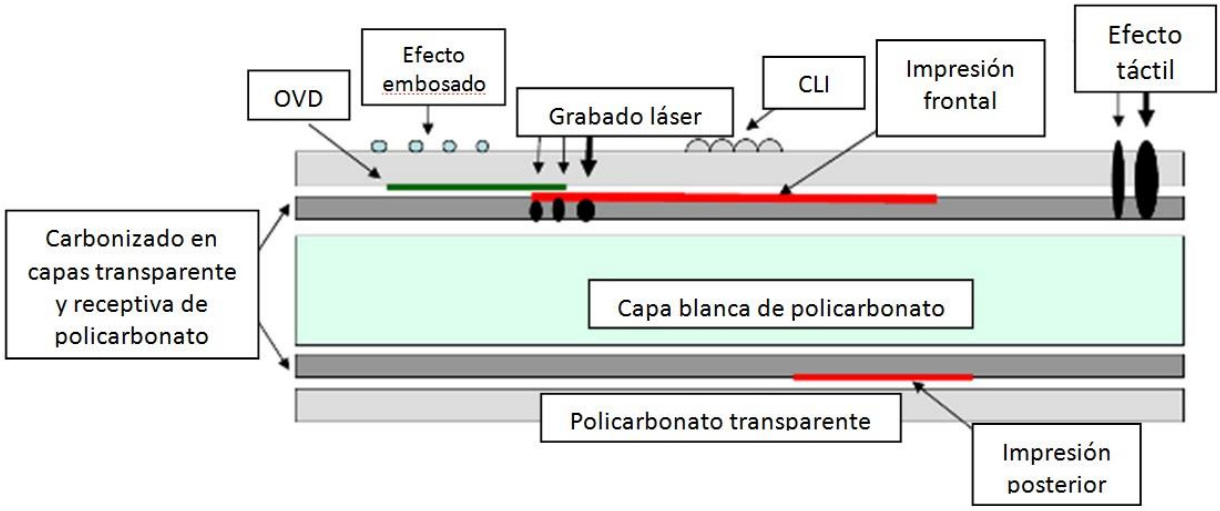


Figura 1 - Estructura de capas de policarbonato de la tarjeta del DNIe

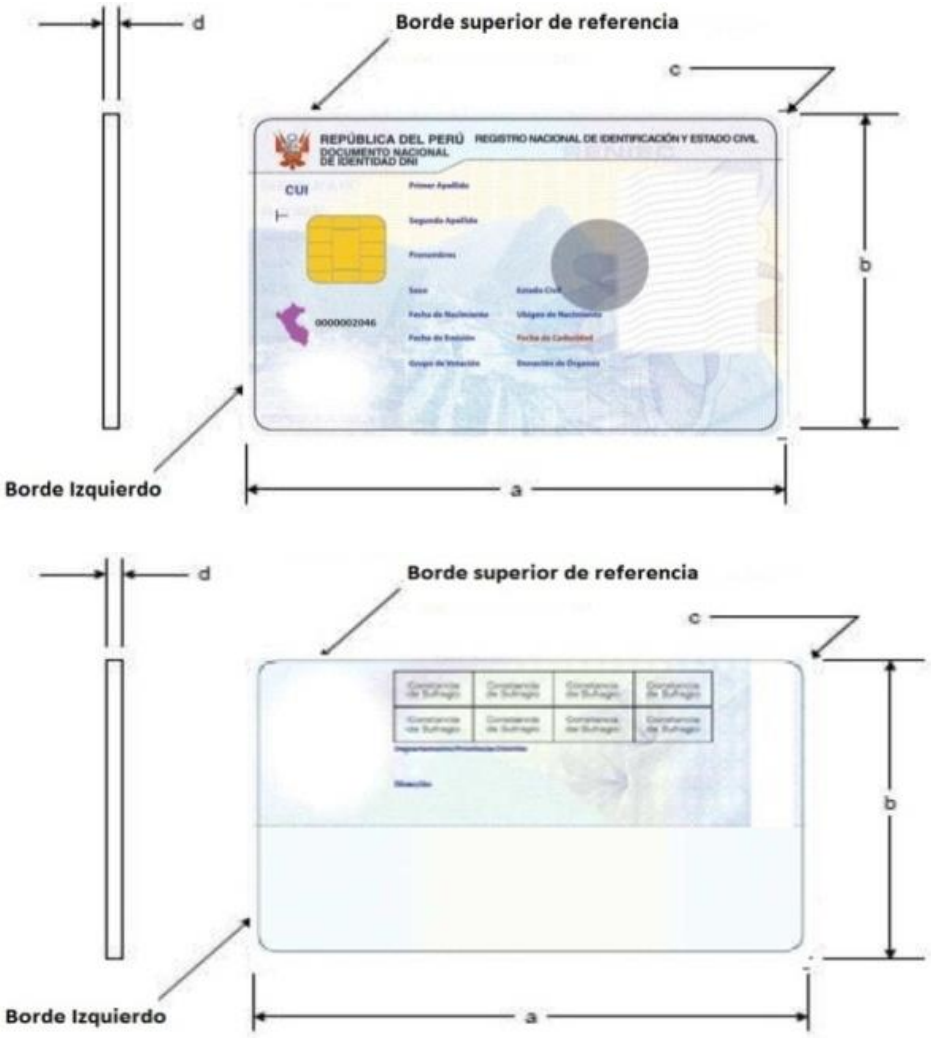
La tarjeta de policarbonato así constituida, posibilita la personalización de texto e imágenes mediante grabado láser en un solo paso. Al estar contenidas todas sus características de seguridad en la propia tarjeta, se evita la complejidad de paso ulterior alguno, como sería por ejemplo la laminación que se practica en el DNI azul actual.

Complementariamente a la seguridad auto contenida de las tarjetas, es importante acotar que el RENIEC ha implementado el Centro de Personalización del DNIe, cumpliéndose en el mismo con exigentes prácticas de seguridad inherentes al manejo de tarjetas inteligentes, de manera que resulte muy poco probable su sustracción, la producción de documentos con falsa identidad o un siniestro. Ello concierne a los sistemas informáticos para la transferencia de datos, el uso de módulos de hardware de seguridad HSM para el almacenamiento de claves de producción, el control de acceso del personal, el control del flujo de la producción, la video-vigilancia, el almacenamiento y control de inventarios de tarjetas, el sistema contra incendios y el acondicionamiento de ambientes.

2.2 Dimensiones y diseño gráfico del DNIe

Dimensiones de la tarjeta

Las dimensiones y tolerancias son las definidas en la norma ISO/IEC 7810 para el formato estándar de tarjeta ID-1, a saber:



	A máx	A min	B máx	B min	C máx	C min	D máx	D min
ID-1	85,90	85,47	54,18	53,92	3,48	2,88	0,84	0,68

Tamaños expresados en mm

Figura 2 - Dimensiones del Documento Nacional de Identidad Electrónico (Anverso y Reverso).

Posicionamiento de las imágenes y texto en el anverso

Figura 3 - Posición de las imágenes (Anverso).

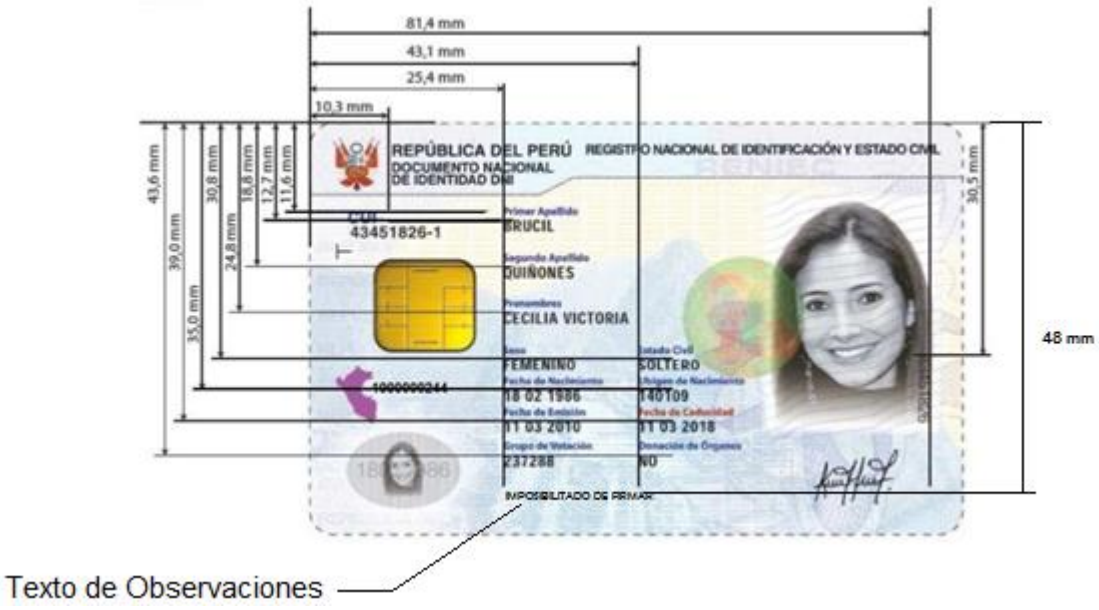


Figura 4 - Posición del texto (Anverso).

Posicionamiento de las imágenes y texto en el reverso

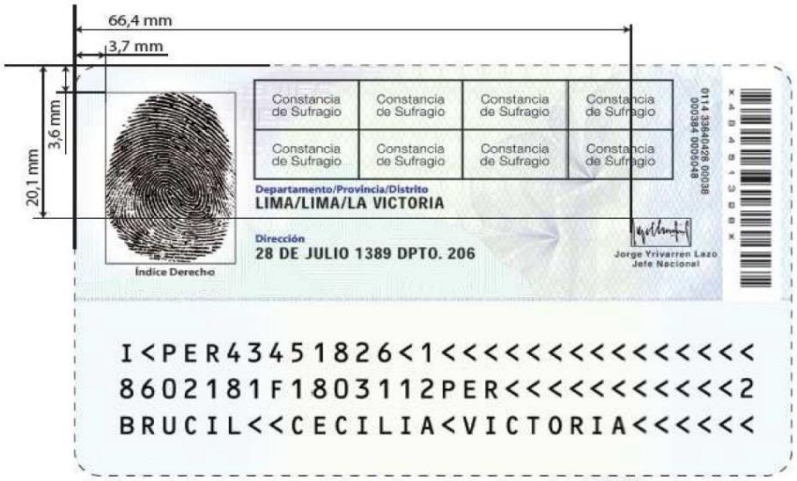


Figura 5 - Posición de las imágenes (Reverso).

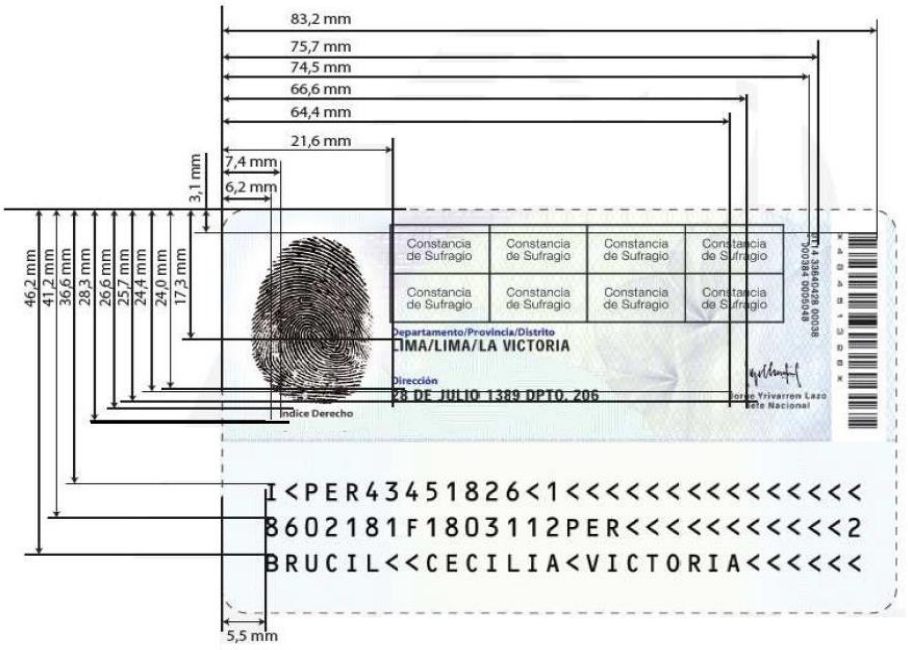


Figura 6 - Posición del texto (Reverso).

2.3 Elementos de seguridad

Un elemento de seguridad es aquel que estando integrado a la estructura física de la tarjeta DNI, y poseyendo características visuales destacables, hace posible al inspector del documento discernir sobre su legitimidad. Los elementos de seguridad de tecnología avanzada, son resultado

de investigación de los fenómenos de difracción de la luz, o del comportamiento óptico de cristales contenidos en líquidos.

Su fabricación requiere de métodos especiales de tratamiento de materiales, usando instrumentos de sofisticado diseño, que están protegidos por patentes internacionales y que implican altos costos. Los elementos de seguridad pueden agruparse bajo las siguientes variantes:

- Textos impresos con Láser. Altamente durable, inmune a adulteración:
  La impresión de textos sobre policarbonato se hace por acción de rayos laser sobre capas subyacentes del material, realizable con equipo de compleja fabricación, como el que RENIEC posee, bajo estrictas medidas de seguridad.
- Diseños numismáticos integrados en capas intermedias del material de la tarjeta: se han aplicado las técnicas de impresión gráfica de los billetes de dinero, como los patrones Guilloche de intricado diseño o micro-textos observables con lupa o con microscopio.
- Dispositivos ópticos incrustados: Cambian de aspecto visual y no son duplicables.
  Corresponden a elementos individuales que se han integrado a capas intermedias del material, que aplican principios de alteración de su percepción óptica, dependiendo del ángulo con que se los observe, o del ángulo de incidencia de la luz sobre ellos, o del tipo de luz.

Su falsificación se considera improbable en un período de al menos 5 años, considerando el avance normal de la tecnología, y el principio óptico que aplican, o de la disponibilidad de la patente, o de los equipos de fabricación, o de la copia de las propiedades gráficas. Son diversas las condiciones que deberían conjugarse, además del costo que representa su fabricación.

El DNIe dispone de elementos de seguridad de tres niveles, los que conceptualmente se describen a continuación:

- Bajo el nivel 1 se consideran los elementos de seguridad cuyas propiedades destacables, inusuales o insólitas, pueden distinguirse a simple vista, sin equipo o herramientas especiales, como por ejemplo el cambio de color de un detalle, o la conversión de un rasgo en otro diferente, o su aparente movimiento, dependiendo del ángulo de visión.
- En el nivel 2, para la observación de la propiedad insólita del elemento de seguridad se requiere de dispositivos simples no especializadas de bajo costo, como podría ser una lupa

para observar microtextos o luz ultravioleta para distinguir figuras no visibles a la luz natural. Este tipo de inspección suele efectuarla personal entrenado.

- En el nivel 3, los elementos de seguridad suelen ser secretos y conocerse solo por el ente emisor del documento de identidad y por los organismos de seguridad. Su inspección puede requerir o no del uso de herramientas o instrumentos. Este tipo de inspección suelen efectuarla peritos.

La elección de los elementos de seguridad para el DNIe se ha hecho teniendo en cuenta el contrarrestar las amenazas conocidas contra un documento de identidad efectuando el mapeo correspondiente buscando seguir los criterios dados por la *American Association of Motor Vehicle Administrators (AAMVA)* en su estándar *Personal Identification – AAMVA North American Standard – DL/ID Card Design.* Un resumen de aquellos incorporados en el anverso del documento puede observarse en la ilustración a continuación:

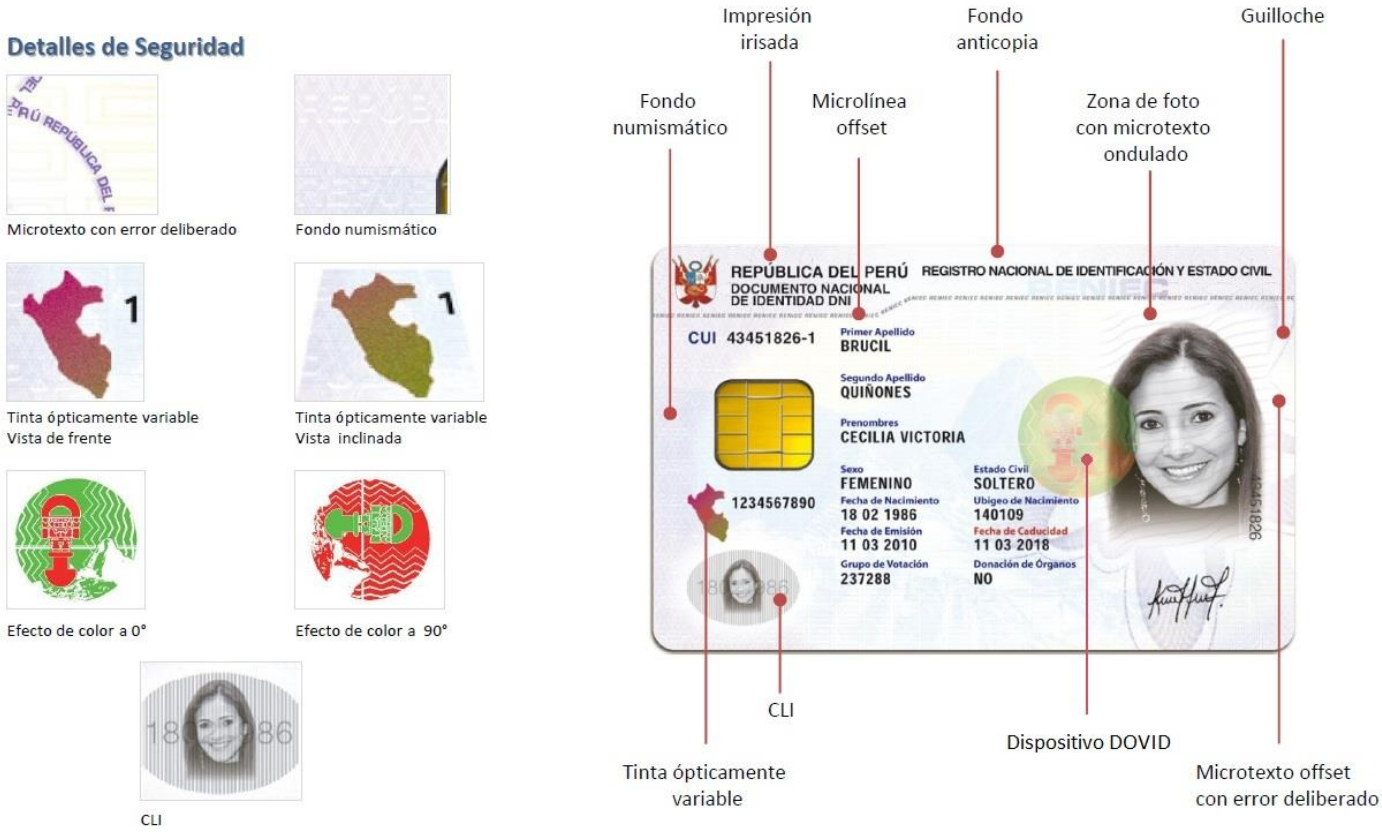


Figura 7 – Elementos de seguridad más importantes en el anverso de la tarjeta

(Fuente: Oberthur Technologies)

Grabado láser de textos sobre policarbonato

La fecha de nacimiento grabada en relieve sobre el anverso (Nivel 1), se logra mediante la regulación de la intensidad del haz láser de la impresora, de modo tal que la superficie del

policarbonato en la capa exterior se quema elevándose a lo largo del delineado del caracter. La superficie de la tarjeta presenta una rugosidad o relieve detectable al tacto.

No es posible producir similar efecto en tarjetas de plástico (PVC). Sólo el policarbonato es apto para ese proceso de grabado, y debe efectuarse con impresoras de alto costo. La impresora que RENIEC opera para la impresión de datos personales en el DNIe y las tarjetas sin personalizar se mantienen bajo estrictas medidas de seguridad.

Diseño numismático: patrón Guilloche

El patrón Guilloche, consiste en finas líneas entretejidas de diseño abstracto (nivel 1), con apariencia de encaje o de pliegues que se desarrollan sobre la superficie cambiando de aspecto, al estilo de billetes de dinero. Este impreso es parte del patrón de fondo, integrado al diseño gráfico de la tarjeta. El DNIe presenta zonas con patrón Gilloche tanto en el anverso como en el reverso.

El diseño es logrado mediante software de computadora de código reservado, y es prácticamente imposible de imitar considerando los cambios graduales de curvatura y color de las líneas que lo conforman.

Diseño numismático: microtexto

El microtexto impreso es sólo legible con ayuda de lupa (nivel 2). A simple vista estos elementos aparentan líneas rectas o quebradas, pero al observarlos con lupa del orden de 10 aumentos, se reconocen textos impresos. En el anverso, el microtexto ubicado en el encabezado consiste en la sigla “RENIEC” repetida a todo lo largo. En el reverso se lee en microtexto “REPUBLICA DEL PERU”, también de manera repetida.

La impresión de microtextos requiere de equipos de impresión de alta precisión que no están fácilmente disponibles por su elevado costo. Adicionalmente, su impresión sobre policarbonato requiere de técnicas de producción muy elaboradas.

Dispositivos ópticos incrustados reconocibles a simple vista: OVI, CLI y DOVID

Se puede apreciar la ubicación y designación de cada dispositivo dentro de la disposición general de la tarjeta en el anverso. En el reverso no se cuenta con dispositivos ópticos reconocibles a simple vista (nivel 1).

El funcionamiento de estos dispositivos se encuentra detallado en los puntos subsiguientes. Los elementos OVI y DOVID son productos fabricados para el DNIe por proveedores especializados con propiedades singulares para resistir el proceso de fusión de las capas del policarbonato al momento de ser integrados en capa intermedia de la tarjeta. El contenido en texto e imagen del CLI se produce por grabado láser sobre la superficie lenticular en la tarjeta de policarbonato ya terminada.

Tratándose de dispositivos ópticos que involucran el reconocimiento de imágenes y/o colores cambiantes, es posible que algunas personas no tengan habilidad para reconocer algunos de ellos, y en tal caso tendrán al resto de dispositivos como alternativa para validar el documento. Es poco probable que una persona con correcta visión y tacto presente dificultad para reconocer los tres dispositivos. Tal criterio ha sido adoptado en la mayoría de países que emiten documento electrónico de identidad en tarjeta de policarbonato, donde por lo general se incluyen tres dispositivos de naturaleza similar a los que tiene el DNIe peruano.

La siglas OVI, significan *"Optically Variable Ink",* o tinta ópticamente variable. El elemento OVI es de nivel 1 y consiste en tinta de cristal líquido depositada en una lámina intermedia del agregado de capas de policarbonato. Los cristales tienen la propiedad de reflejar luz de diferente longitud de onda en distintos ángulos de reflexión. Ello se percibe como un cambio de color del elemento al cambiar el ángulo de visión de la tarjeta en cualquier sentido: horizontal, vertical o diagonal.

Existen productos que exhiben el efecto tornasol cuando se los observa en diferentes ángulos de visión, pero no tienen el grado de precisión en el ángulo con que se puede percibir, ni la luminosidad que tiene el OVI del DNIe.

La siglas CLI significan *"Changeable Laser Image",* o imagen (grabada con) láser cambiante, constituyendo un elemento de seguridad de nivel 1. En la fase de pre-personalización, el proveedor de la tarjeta graba diminutos surcos sobre un área reducida de su superficie, formando

una estructura difractiva de la luz que actuará como lente discriminador de las imágenes de foto fantasma y fecha de nacimiento del ciudadano que posteriormente se graban en la capa subyacente. De este modo, esas dos imágenes diferentes grabadas a láser en el mismo lugar de la tarjeta se hacen nítidas o se opacan alternativamente cuando la tarjeta es inclinada a la derecha o a la izquierda.

El espesor, profundidad y separación de los surcos sobre el policarbonato es del orden de décimas de milímetro. Esta precisión únicamente se logra con equipos industriales de especial fabricación y alto costo sólo operados por los fabricantes de tarjetas inteligentes.

Las siglas DOVID, significan *"Diffractive Optically Variable Image Device",* o dispositivo de imagen ópticamente variable por difracción, por sus siglas en inglés. Los DOVIDs exhiben una variedad de imágenes y patrones complejos, dependiendo del ángulo de visualización (o sea si ellos son rotados o inclinados), basados en la difracción de la luz natural.

El DOVID del DNIe usa la tecnología denominada DID, de difracción de orden cero, cuya rejilla de nanoestructura es originada mediante rayo láser, ofreciendo una gran capacidad de diferenciación de color. Se observa la permutación de dos colores, rojo o verde, según áreas elegidas del diseño gráfico. Estas áreas intercambian su color cuando se rota 90° el dispositivo sobre su mismo plano. La producción de difracción de orden cero, es observable tanto con fuente de luz puntual como con luz difusa. Además, es altamente transparente, muy apropiado para sobreponerlo sobre textos o imágenes, en el caso del DNIe específicamente sobre la fotografía.

El DID es producido mediante un proceso químico-industrial muy complejo que requiere equipamiento especializado resultando muy difícil de imitar. Por su aplicación mediante estampado en caliente sobre una capa de policarbonato, la nanoestructura DID está incrustada dentro del material de manera inaccesible y no puede ser alterada.

El efecto de movimiento hacia los costados de las líneas quebradas multicolores que flanquean a la imagen Tumi es logrado al observar el elemento mientras se inclina la tarjeta hacia adelante y hacia atrás. Esta propiedad se debe a otra tecnología incluida en el DOVID incorporado en el DNIe denominada microlitografía interferencial, la que produce efectos difractivos muy luminosos.

Finalmente, al observar el DOVID a través una lupa se hace visible la lectura del microtexto “REPUBLICA DEL PERU” que corre horizontalmente por la parte media del círculo del elemento. Esta impresión es realizada con técnicas gráficas avanzadas sobre el material transparente del elemento.

Dispositivos ópticos incrustados reconocibles bajo luz ultravioleta

Son imágenes visibles utilizando una lámpara de luz ultravioleta (UV). Estas imágenes se han impreso por el lado interior de las capas de policarbonato que recubren al DNIe (dispositivo de nivel 2), usando tinta especial que es transparente a la luz natural, pero que refleja la luz ultravioleta.

En el lado anverso se observan las siguientes seis (6) figuras:

1) El Cóndor (símbolo Nazca)
2) Escudo Nacional Peruano
3) El Colibrí (símbolo Nazca)
4) El Perro (símbolo Nazca)
5) La Araña (símbolo Nazca)
6) El Mono(símbolo Nazca)

En el lado del reverso, se observan las siguientes tres (3) figuras:

1) El Mono (símbolo Nazca) sobre diseño textil
2) Mapa del Perú
3) El Colibrí (símbolo Nazca)

3. EL CHIP

3.1 Descripción general

El microprocesador, circuito integrado, o “chip” embebido en la tarjeta del DNIe, se compone de hardware y software.

El hardware del controlador electrónico tiene los siguientes componentes: Unidad de procesamiento de Tecnología C-MOS, Memorias de tipo ROM, RAM y EEPROM, Unidad de Administración de Memoria, Coprocesadores para ejecución de algoritmos criptográficos y generación de números aleatorios e Interfaz con contactos ISO/IEC 7816.

El software en el microprocesador comprende el sistema operativo y dos aplicaciones “applets” seleccionables para el programador, además de otras de uso interno. El sistema operativo ID-One-Cosmo-V7 de Oberthur Technologies implementa las especificaciones de JavaCard (versión 2.2.2), administradas por Oracle Corporation (originalmente desarrolladas por Sun Microsystems), lo que implica un entorno de ejecución seguro para las aplicaciones de software que se ejecutan en tarjetas inteligentes, contemplando su limitada capacidad de memoria y procesamiento.
Permite además, que múltiples aplicaciones sean desplegadas en una misma tarjeta, a la vez que nuevas aplicaciones puedan ser agregadas después de haber sido expedida al usuario final.

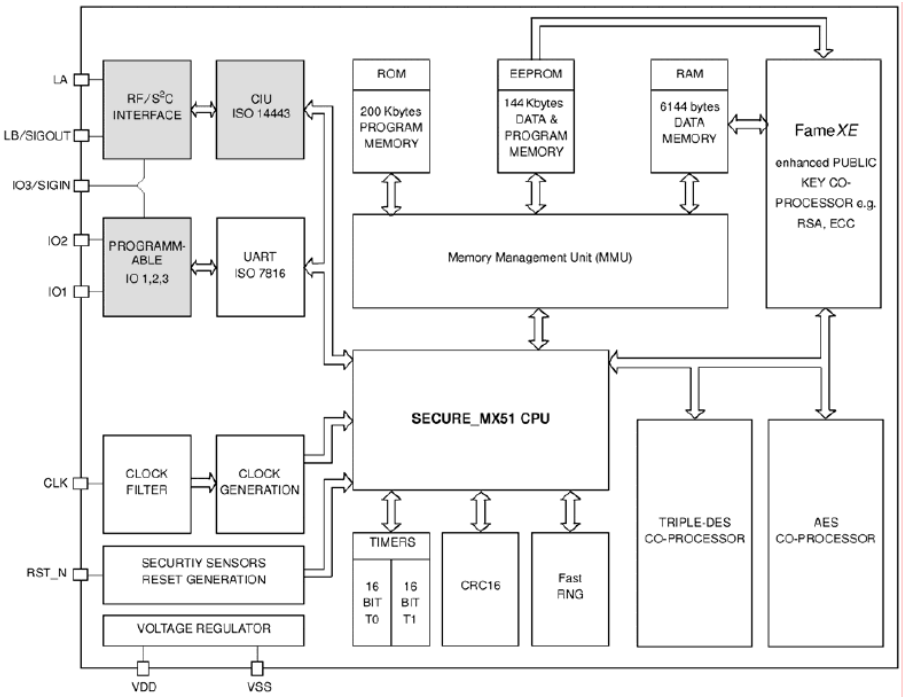


Figura 8 - Diagrama de bloques del Controlador NXP P5CD144V0B para Tarjeta Inteligente (NXP Semiconductors)

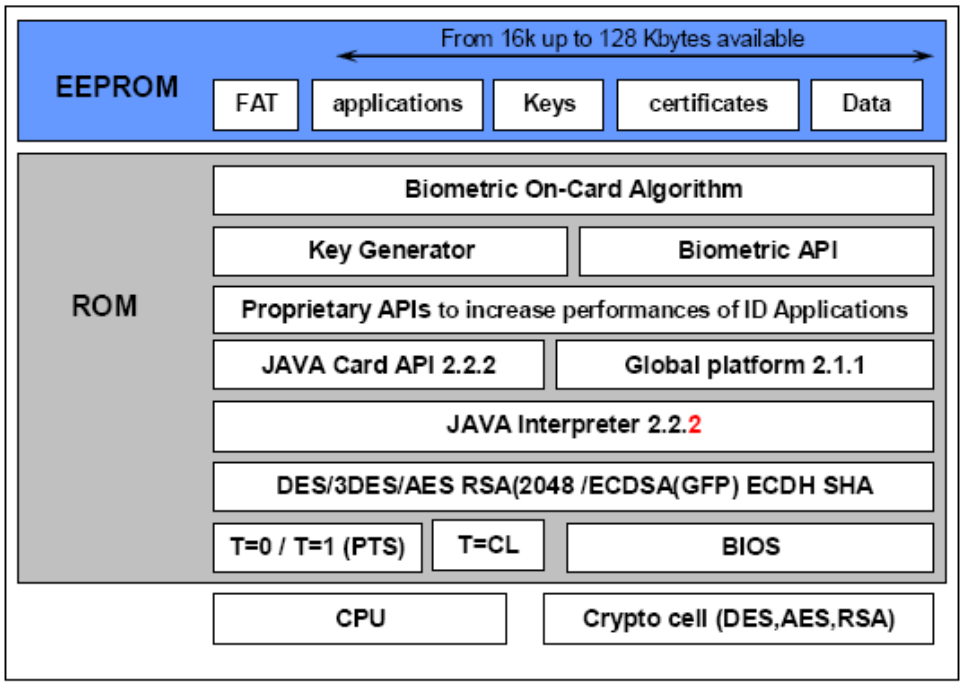


Figura 9 - Diagrama de bloques lógico del sistema operativo ID-One-Cosmo-V7 (Oberthur Technologies)

El objetivo de la tecnología JavaCard es brindar muchos de los beneficios de la programación Java al mundo de recursos reducidos de la tarjeta smart card, los que se resumen en el dicho "programar una vez y ejecutar en todas partes". Tarjetas fabricadas con distintos chips, pero que tienen sistemas operativos JavaCard, pueden ejecutar programas Applet, basados en sintaxis y semántica común. Ello facilita la labor de programación, y no requiere instalar el programa cargado en el chip, previo a su ejecución. Asimismo, facilita la instalación de varios programas en una misma tarjeta para ofrecer servicios distintos (PKI para la firma digital, ICAO para la identificación bajo el estándar de documento de viaje, MOC para la autenticación de la identidad por medios biométricos, etc.).

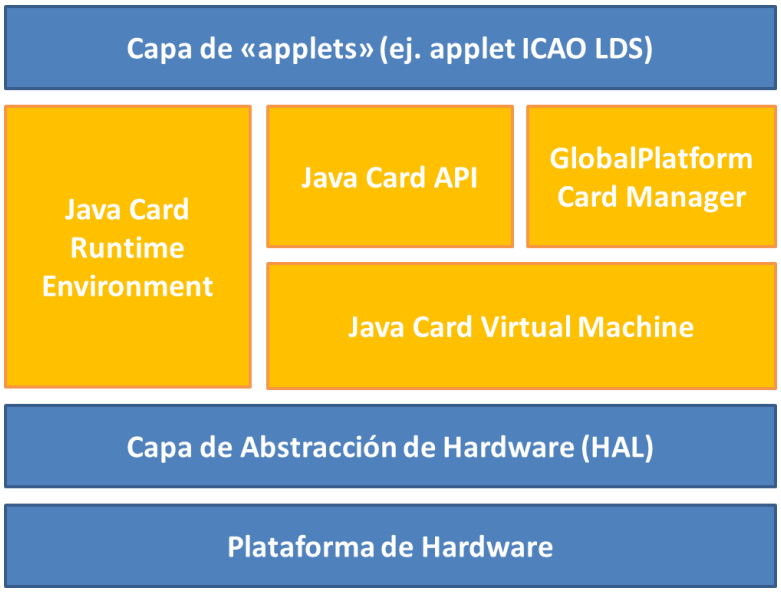


Figura 10 - Componentes JavaCard® en el sistema operativo del DNIe

El sistema operativo implementa también las especificaciones de Global Platform (versión 2.1.1), organismo representativo de diversas entidades comprometidas con el despliegue seguro e interoperable de la tecnología de tarjetas inteligentes, en aplicaciones de pago, de telefonía móvil, de identificación nacional, de recaudación de tarifas en tránsito, o atenciones de salud, a nivel mundial.

Tanto el hardware como el software, están fabricados con el objetivo de mantener altos niveles de seguridad contra intrusiones. En particular, la aplicación PKI implementa un código (PIN) que el usuario debe ingresar para activar la realización de firma o autenticación digital. El ingreso de código erróneo por tres veces consecutivas produce el bloqueo de la aplicación, la cual sólo puede reactivarse con intervención del RENIEC.
Estas características del chip, confieren al DNIe su calidad de almacén seguro para los datos, las plantillas biométricas de huellas dactilares, las claves privadas de los certificados digitales y otras claves. Por otro lado, los procedimientos criptográficos relacionados con la autenticación, o firma digitales o de cotejo para verificación biométrica, son realizados internamente en el chip, de modo tal que los valores secretos de claves o plantillas biométricas, nunca son presentados al exterior.

3.2 Certificaciones

El software Sistema Operativo ejecutado en el microprocesador del DNIe, posee certificación de cumplimiento de los requerimientos funcionales de seguridad establecidos por el estándar Common Criteria, con nivel de evaluación EAL 5+, y posee también certificación de cumplimiento

del Estándar Federal de Procesamiento de Información FIPS 140-2 nivel 3 de los Estados Unidos de Norte América como módulo criptográfico.

Los Criterios Comunes (CC) son resultado de la armonización de criterios sobre seguridad de productos software, utilizados por diferentes países. Los CC permiten comparar los resultados entre evaluaciones de productos independientes. Para ello, se establece un conjunto común de requisitos funcionales para los productos hardware, software o firmware. El proceso de evaluación determina un nivel de confianza, o grado, en que el producto satisface la funcionalidad de seguridad de esos productos, y ha superado las medidas de evaluación aplicadas. La lista de productos certificados según los CC se encuentra disponible en la página web de Common Criteria.

El proceso de evaluación implica la verificación de que un producto software específico cumple con los siguientes aspectos:

- Los requisitos del producto están definidos correctamente.
- Los requisitos están implementados correctamente.
- El proceso de desarrollo y documentación del producto cumple con los requisitos de determinado nivel de seguridad establecidos bajo los denominados EAL (Evaluation Assurance Level).

Los niveles de seguridad son los definidos en el estándar ISO/IEC 15408-3, y van desde el nivel EAL 1 (el más bajo) hasta el EAL 7 (el más alto). Cada uno de los niveles se asocia con un conjunto de medidas o prácticas seguidas en el desarrollo del producto, indicativas de la profundidad y rigor de la evaluación y que son verificadas de manera acumulativa. Es decir, que la verificación de un nivel implica que se han verificado también los niveles inferiores.

El estándar de procesamiento de información federal (FIPS) es un conjunto de requerimientos de seguridad para módulos criptográficos. Existen cuatro niveles de seguridad definidos, que van desde el Nivel 1 (el más bajo) hasta el Nivel 4 (el más alto), así como también diversas certificaciones específicas dentro del estándar. Cada nivel alcanza la más alta concentración de ciertos criterios considerados por el gobierno federal de los Estados Unidos, dependiendo del nivel de seguridad y la calidad de pruebas requeridas específicamente para el producto.

Las áreas de certificación más destacadas incluyen:

- Diseño Básico
- Documentación
- Medidas de seguridad física
- Algoritmos criptográficos
- Interfaces

Por su parte, el Instituto Nacional de Estándares y Tecnología (NIST) revisa los estándares FIPS cada cinco años, y estos estándares han sido implementados por distintos fabricantes y adoptados por diversos gobiernos en el mundo.

Un módulo criptográfico certificado FIPS140-2 Nivel 3, alcanza uno de los más altos niveles de seguridad, con encriptación en hardware de grado militar, protección contra ataques de estrés (de fuerza bruta), y un alto rendimiento en procesamiento.

4. FUNCIONALIDADES Y USOS

Basado en sus recursos de procesamiento informático, el DNIe implementado cuenta con las siguientes funcionalidades:

- Interacción con sistemas electrónicos de validación de identidad basados en el estándar de la Organización de Aviación Civil Internacional, ICAO por sus siglas en idioma inglés, con la salvedad que el DNIe requiriere para ello de un lector de interfaz de contactos y no uno sin contactos
- La firma digital de documentos cuyos resúmenes “hash” se presenten al DNIe. Para esta operación se usa la clave privada generada y resguardada en su chip, además del certificado digital de firma otorgado por RENIEC y almacenado también en el chip del DNIe.
- Ejecutar la autenticación digital de la identidad de manera semejante a la firma digital. Para esta operación, se usa la clave privada generada y resguardada en su chip, además del certificado digital de autenticación otorgado por RENIEC y almacenado también en el chip del DNIe.
- Permitir que aplicaciones externas almacenen o extraigan datos, en o de cuatro estructuras de datos predefinidas a manera de registros de información básica. Dichas estructuras están diseñadas para almacenar, por ejemplo, datos de identificación, de salud, de

subvenciones en programas sociales o de constancias de sufragio. El acceso a estas estructuras está restringido mediante claves establecidas según políticas definidas.

- Producir la verificación biométrica de la impresión dactilar presentada a un lector biométrico y, consecuentemente, de la identidad del titular. Para esta operación, denominada “Match-on-Card”, el DNIe realiza la comparación de la plantilla de la huella dactilar generada mediante el lector y el algoritmo de extracción de minucias con la del titular que se encuentra almacenada en su memoria.

Para poder utilizar estas funcionalidades el DNIe deberá estar conectado a un computador con el correspondiente lector de tarjetas inteligentes de contacto. Podrá requerirse también de un lector de huellas dactilares en el caso de la funcionalidad de verificación biométrica.

4.1 Funcionalidad de identificación ICAO

Comprende la funcionalidad de documento de viaje eMRTD conforme se especifica por la Organización de Aviación Civil Internacional ICAO en su Doc 9303, Parte 3, Volumen 2, 2008, no obstante, al no disponer el DNIe de interfaz sin contactos la lectura de los datos deberá hacerse a través de la interfaz de contactos.

Figura 11 - Aplicación para documentos de viaje de ICAO integrada en el DNIe

- Ejecuta los métodos especificados por ICAO:
  - Autenticación pasiva,
  - Autenticación activa, y
  - Control de acceso básico
- Implementa la estructura lógica de datos (LDS) definida por ICAO, que abarca 16 grupos de datos. El DNIe tiene contenido en los grupos de datos siguientes:

- El grupo de datos 1 incluye:
  - Tipo de documento
  - País o Entidad emisora
  - Nombre del titular
  - Número del documento con dígito de control
  - Nacionalidad
  - Fecha de nacimiento con dígito de control
  - Sexo
  - Fecha de expiración con dígito de control
  - Dígito de control compuesto
- El grupo de datos 2 contiene codificación de la imagen del rostro del ciudadano, en formato JPEG2000.
- El grupo de datos 7 contiene codificación de la imagen de la firma manuscrita o rúbrica del ciudadano, en formato JPEG2000.
- El grupo de datos 12 contiene los siguientes datos de documento adicionales:
  - Autoridad emisora
  - Fecha de emisión
- El grupo de datos 15 contiene la clave pública para la autenticación activa.

4.2 Funcionalidad PKI

Esta funcionalidad comprende los métodos criptográficos aceptados en la Infraestructura de Clave Pública PKI para el manejo de los certificados digitales, realización de la firma y la autenticación digital y generación, custodia y acceso a las claves secretas almacenadas.

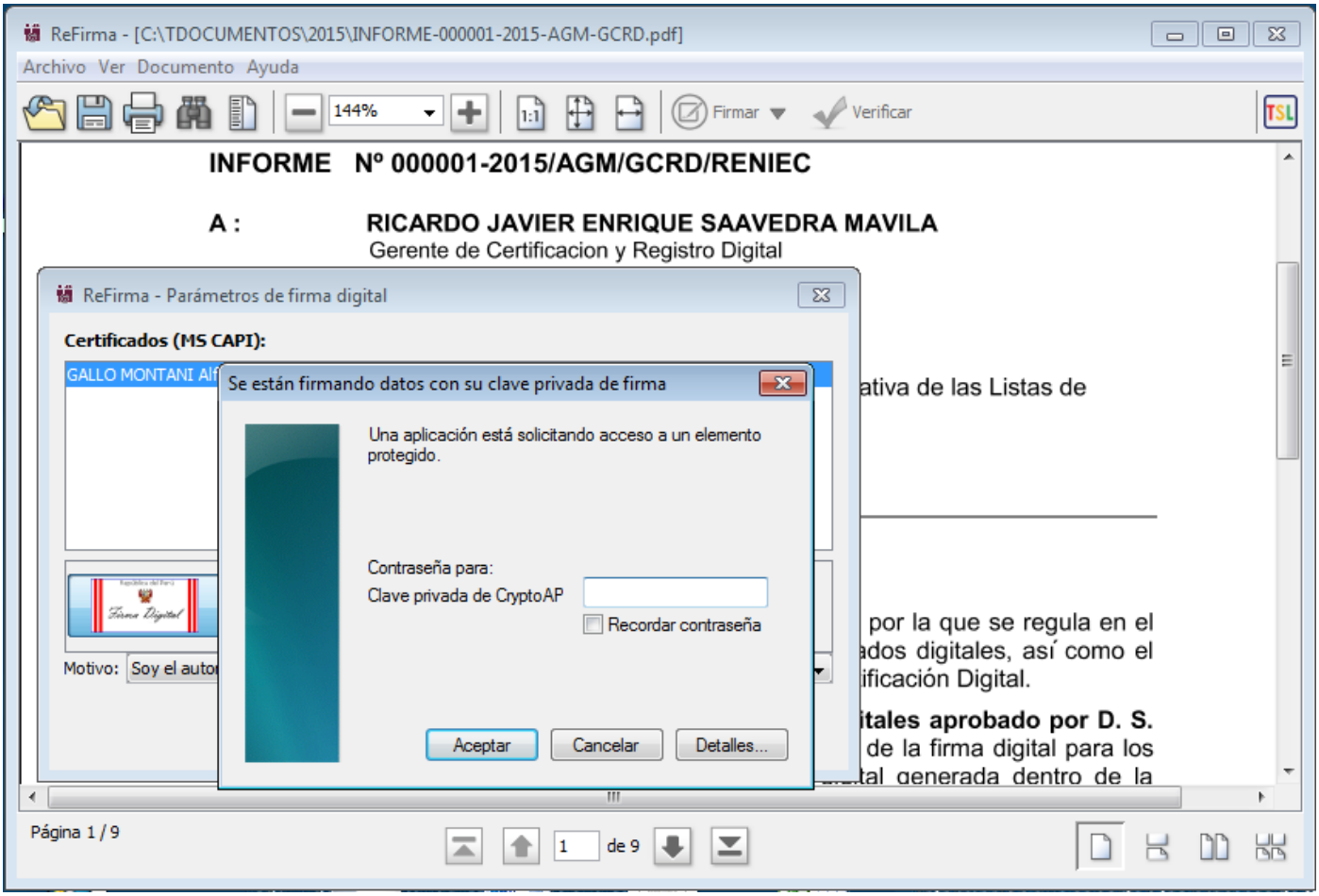


Figura 12 - Firma digital en aplicativo ReFirma del RENIEC

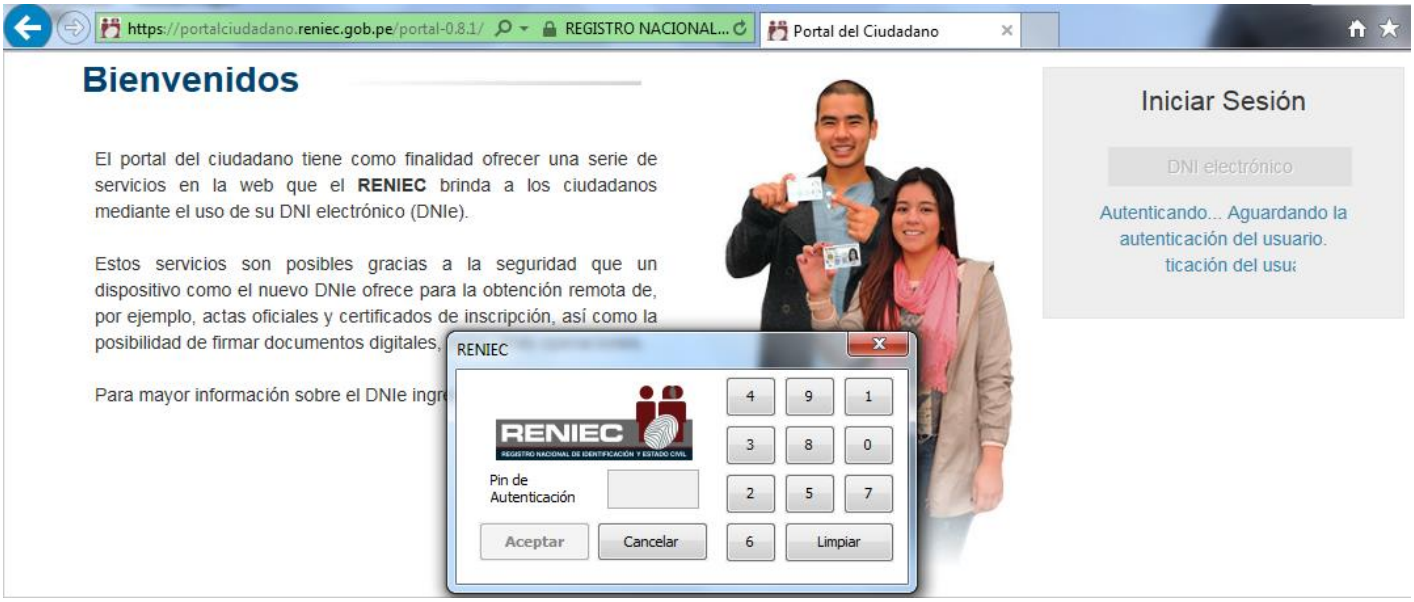


Figura 13 - Autenticación mediante certificado digital, acceso al portal ciudadano del RENIEC

Se refieren a continuación las tareas ejecutables por la aplicación PKI:

- Genera y maneja claves de cifrado asimétrico RSA de hasta 2048 bits, y ejecuta el cifrado y el descifrado correspondientes.
- Genera y maneja claves de cifrado simétrico DES de 64 bits, 2DES de 128 bits, 3DES de 192 bits, y AES de hasta 256 bits, y ejecuta el cifrado y el descifrado correspondientes.
- Ejecuta funciones criptográficas de resumen en algoritmos de Hash Seguro SHA-160, SHA-256, SHA-384, SHA-512, aplicadas a procedimientos de autenticación digital.
- Tiene almacenadas cuatro claves simétricas 2DES de 128 bits, a ser operadas por aplicaciones externas en la lectura o escritura de datos del ciudadano bajo cuatro estructuras implementadas.
- Tiene almacenadas dos claves RSA privadas de 2048 bits, asignadas a sendos certificados digitales aplicados en la Autenticación o la Firma digital. Cada una de estas claves tiene asociado un número de identificación personal PIN, que al ser ingresado por el ciudadano, invoca la realización de la autenticación o de la firma digital, según corresponda.
- Almacena los certificados digitales para autenticación y para firma digital, además de los certificados de la cadena de confianza que corresponden a las entidades de certificación intermedia y raíz.
- Implementa contadores de intentos erróneos para el ingreso de los números personales de identificación PIN, asociados a la realización de la autenticación o la firma digital. Al completarse tres intentos erróneos consecutivos, el acceso al uso del PIN queda bloqueado y sólo puede ser recuperado con intervención del RENIEC.
- Almacena las plantillas biométricas de dos huellas dactilares del ciudadano, para ser usadas como credencial para la generación y activación o desbloqueo del número PIN a manera de un PUK *(PIN Unblock Key).* Con intervención del RENIEC, tales plantillas son cotejadas con la plantilla biométrica capturada de la huella dactilar del ciudadano, arrojando el resultado sobre su reconocimiento. De ser positivo, procede la activación del número PIN para el ciudadano, y en caso de ser negativo no es posible activar el PIN.
- Para aquellos ciudadanos que RENIEC considere no elegibles para verificación biométrica dactilar, la aplicación PKI provee la asignación de un código clave personal de desbloqueo PUK, el que cumple una función similar al posibilitar la generación y activación del número PIN cuando su valor es invocado por el ciudadano en las instalaciones del RENIEC.
- El applet PKI se adhiere al estándar ISO/IEC 7816, en sus partes:
  - Parte 4.- Estructura de comandos APDU.

- Parte 5.- Asignación de números de identificación de aplicaciones.
- Parte 6.- Definición de propiedades de los elementos de datos usados para intercambio de aplicaciones.
- Parte 8.- Especificación de comandos para operaciones de seguridad.
- Parte 9.- Comandos para la administración de la tarjeta y sus archivos.
- Parte 15.- Aplicación de Información Criptográfica.

• Implementa cuatro estructuras de datos destinadas al almacenamiento de información del ciudadano. El applet PKI provee acceso a lectura, modificación o escritura en las mismas mediante procedimientos con claves simétricas. Las estructuras pueden utilizarse para almacenar, por ejemplo:
  - Datos de identidad del ciudadano, conforme lo hace ya el RENIEC en la denominada Aplicación Básica de Identidad, ABI.
  - Constancias de votación para procesos electorales.
  - Subvenciones percibidas en programas sociales.
  - Datos de salud en lo referido a emergencias, vacunas y transfusiones.

4.3 Funcionalidad biométrica *Match on Card*

El DNIe incorpora la tecnología de verificación biométrica de huellas dactilares, realizable mediante procesamiento informático en el chip. Las funcionalidades para esta aplicación dependen fundamentalmente de tres componentes cuales son el motor biométrico, el API biométrico y un applet biométrico. No obstante, el acceso a las mismas se hace a través del applet PKI para lo cual debe seleccionarse previamente.

En la etapa de personalización del documento DNIe, además de los datos textuales y foto del ciudadano, se almacenan también las plantillas o códigos extractos de rasgos biométricos (minucias) de las huellas dactilares de ambos dedos índices. La fuente para la producción de esas plantillas son las imágenes de huellas registradas en la Base de Datos del RENIEC. La aplicación *Match-On-Card* utiliza esas plantillas almacenadas como referencia para la comparación con los códigos capturados directamente de los dedos del ciudadano y que son presentados al DNIe por la aplicación cliente ejecutada en el computador dedicado a la inspección del documento.

- Ejecuta el enrolamiento de hasta dos plantillas de impresiones dactilares, en el formato definido para tarjetas inteligentes por ISO/IEC 19794-2, *"Compact Size Finger Minutiae Card Format".*
- La aplicación PKI almacena las plantillas biométricas en un segmento protegido de memoria, sin acceso de lectura ni escritura posterior.
- Si la verificación biométrica resulta exitosa el estado de seguridad de la tarjeta es actualizado y una señal apropiada es enviada al sistema inspector externo.
- El funcionamiento del applet *Match on Card* depende del applet PKI dado que este último debe seleccionarse antes de enviarle comandos. El applet PKI controla también al contador de intentos erróneos en su uso como credencial y le brinda acceso a las plantillas biométricas.
- El applet *Match on Card* se adhiere al estándar ISO/IEC 7816, en sus partes:
  - Parte 4. Estructura de comandos APDU.
  - Parte 11. Uso de comandos y objetos de datos para verificación personal por métodos biométricos.

PARTE II

COMANDOS APDU PARA EFECTUAR OPERACIONES CON EL DNI ELECTRÓNICO

I. OPERACIONES

Las diferentes operaciones que se pueden realizar con el DNI electrónico (DNIe) requieren de la ejecución de secuencias de comandos[1], las cuales pueden ser agrupadas en:

1. Obtención de Certificados:

Los certificados de la estructura lógica PKI del DNIe pueden ser obtenidos mediante la siguiente secuencia de comandos básicos:

i. Iniciar contexto PKI
ii. Seleccionar el Master File
iii. Seleccionar el DF de la estructura PKI
iv. Seleccionar el EF del certificado de interés (EF-340X - y extraer el tamaño del certificado)
v. Leer el contenido del certificado previamente seleccionado

Nota: EF-340X hace referencia a los EFID listados en la Estructura lógica PKI

2. Firma de Hash con clave privada:

La firma de un arreglo de bytes suministrado (HASH) con las claves privadas de Autenticación o Firma se obtiene siguiendo la secuencia de comandos básicos:

i. Iniciar contexto PKI
ii. Verificar PIN de la credencial de X.
iii. Establecer el MSE, para la clave privada de X.
iv. Ejecutar el PSO, con los bytes que se desean firmar (HASH).
v. Recuperar los bytes firmados.

Nota: Donde (X) representa a la (credencial o clave privada) de (Autenticación o Firma).

3. Creación de un canal seguro SMA:

La generación de un canal seguro SMA se obtiene siguiendo la secuencia, “que implementa el protocolo de intercambio de claves”, que es mostrada a continuación:

i. En el DNIe. Generación del par de claves SMA.
ii. En el DNIe. Obtener desafío (Mensaje de Control, Clave Maestra).
iii. En el terminal. Generar claves de pre-sesión (ENC, MAC).
iv. En el terminal. Generar bloque que contiene las claves de pre-sesión y el mensaje de control con las reglas del formato PKCS#1 Tipo 2, y cifrar el bloque creado con la clave pública SMA.
v. En el DNIe. Autenticación General del bloque cifrado, y generar las claves de sesión (ENC, MAC).
vi. En el terminal. Generar las claves de sesión (ENC, MAC) utilizando la clave Maestra.

[1] Esta sección del documento asume conocimiento previo de conceptos de protocolos de comunicaciones y tarjetas inteligentes.

4. Verificación biométrica (Match on Card - MoC):

El DNIe contiene la información de las plantillas biométricas de las huellas dactilares del ciudadano. La verificación biométrica requiere como mínimo, la siguiente secuencia de pasos.

i. En el terminal. Captura de la huella dactilar del ciudadano y extracción de las plantillas biométricas en el formato ISO/IEC 19794-2 Compact Size Finger Minutiae Card Format
ii. En el DNIe. Iniciar contexto PKI
iii. En el DNIe. Verificación biométrica de la huella dactilar capturada

5. Obtención de datos básico del ciudadano:

El DNIe contiene una estructura de datos lógica especificada por la Norma ICAO. Esta estructura contiene datos básicos del ciudadano y otros organizados en grupos, elementos comunes y de seguridad. La lectura de estos datos se obtiene realizando la siguiente secuencia de pasos.

i. Realizar un BAC para el establecimiento de un canal seguro de comunicación
ii. Autenticación pasiva
iii. Autenticación activa (opcional)
iv. Lectura de los grupos de datos habilitados utilizando mensajería segura a través del canal seguro

Nota: Los procedimientos para efectuar cada uno de los pasos de esta operación, están descritos en la especificación de la Norma ICAO Doc 9303.

6. Obtención de datos básicos del ciudadano:

El DNIe contiene datos básicos del ciudadano. Estos datos residen en el chip del DNIe, específicamente, en el registro denominado ABI. Para obtener estos datos, se realiza la siguiente secuencia de pasos.

i. Iniciar contexto PKI
ii. Seleccionar el EF del registro ABI
iii. Lectura e Interpretación del registro ABI

Nota: La lectura de estos datos no requiere el establecimiento de un canal seguro.

La especificación técnica de los comandos requeridos en estas operaciones, son descritas en las siguientes secciones.

II. PRELIMINARES

1. Acrónimos

Acrónimos y términos abreviados utilizados en este documento

Siglas	Definiciones
AID	Application Identifier
APDU	Application Protocol Data Unit
CLA	Class byte of an APDU
CRDO	Control Reference Data Object
CRT	Control Reference Template
DF	Dedicated File
EF	Elementary File
EFID	File identifier
FCI	File Control Information
INS	Instruction code
Lc	Length of command data field
Le	Expected length of response data field
MAC	Message Authentication Code
ENC	Encode
MF	Master File
OID	Object Identifier
SMA	Secure Messaging Anonymous
TLV	Tag Length Value
LDS	Logic Data Structure
DG	Data Group
BAC	Basic Access Control
SW1-SW2	Status Word
PKI	Public Key Infrastructure
ICAO	International Civil Aviation Organization

Acrónimos

2. Comunicación con APDUs

La comunicación con APDUs toma como base el modelo *comando-respuesta*, definido en la norma ISO 7816-4. La especificación tiene diferentes formatos para un comando APDU y su correspondiente APDU respuesta.

La estructura general para un comando APDU es:

Cabecera (4 bytes)				Campos opcionales		
CLA	INS	P1	P2	Lc	Data	Le

Estructura de un comando APDU

La cabecera describe el comando que la aplicación ejecuta. Los primeros cuatro bytes del comando APDU representan la cabecera, donde:

CLA	Representa la clase, indicando si el comando es un mensaje conforme al ISO 7816-4
INS	Indica la instrucción
P1, P2	Indica parámetros adicionales

Cabecera de un APDU

Los otros campos del comando APDU son opcionales (lo que significa que ellos pueden estar ausentes en algunos casos). Estos campos definen datos adicionales suministrados con el comando, los cuales son:

Lc	Indica la longitud del campo DATA
DATA	Indica los datos presentes en el comando
Le	Indica la longitud de la respuesta esperada

Campos opcionales de un APDU

Hay cuatro formatos diferentes de comandos APDU, dependiendo si el campo DATA está incluido en el comando y si los datos de la respuesta son requeridos.

Cuando los datos no están presentes en el comando y los datos de la respuesta no son requeridos, entonces el formato del comando APDU es:

CLA	INS	P1	P2

Formato APDU Nº 1

Cuando los datos en el comando no están presentes, pero los datos de la respuesta son requeridos, entonces el formato del comando APDU es:

CLA	INS	P1	P2	Le

Formato APDU Nº 2

Cuando los datos en el comando están presentes, pero los datos de la respuesta no son requeridos, entonces el formato del comando APDU es:

CLA	INS	P1	P2	Lc	DATA

Formato APDU Nº 3

Cuando los datos en el comando están presentes y los datos de la respuesta son requeridos, entonces el formato del comando APDU es:

CLA	INS	P1	P2	Lc	DATA	Le

Formato APDU Nº 4

Las respuestas siempre son requeridas, aún si ellas no contienen datos. La estructura de un APDU respuesta es:

Data	SW1	SW2

Formato APDU Nº 5

La combinación (SW1, SW2), comúnmente llamada *status word,* siempre está presente en la respuesta. Cada combinación tiene una interpretación acorde al último comando APDU procesado.

Para el intercambio de comandos sobre un canal seguro, el tercer bit del parámetro CLA debe ser establecido en 1.

3. Identificador de la tarjeta

La tarjeta responde con el siguiente identificador:

ATR	3BDD18008131FE4580F9A0000000770100700A90008Bh	22 bytes

ATR del smart card – DNIe

4. Identificadores de aplicación

4.1 Instancia PKI

El contexto PKI viene contenido en un paquete con el siguiente identificador de instancia:

AID	A0000000770100700A1000F100000100h	16 bytes

AID de la instancia del contexto PKI del DNIe

4.2 Instancia LDS

El contexto ICAO es establecido con el siguiente identificador en la tarjeta y su longitud es de 7 bytes:

AID	A0000002471001h	7 bytes

AID de la instancia del contexto ICAO del DNIe

5. Estructuras lógicas

5.1 Estructura Lógica PKI

Esta estructura lógica contiene los certificados digitales y los datos públicos contenidos en el DNIe, estos se describen a continuación en la siguiente tabla.

Tipo de archivo	**EFID**	**Descripción**
MF	3F00h	Master File
DF	5015h	DF de la estructura PKI
EF	3401h	Certificado de Autenticación del ciudadano
EF	3402h	Certificado de Firma del ciudadano
EF	3407h	Certificado CA
EF	3408h	Certificado CA Intermedia
EF	FD01h	Registro ABI

Estructura lógica PKI básica del DNIe

5.2 Estructura Lógica de datos ICAO

La norma ICAO especifica como opcional el MF, por tanto el DNIe no implementa un MF. El sistema de archivos contiene un único DF designado como DF1 y es implícitamente seleccionado cuando la aplicación LDS es seleccionada. La estructura de datos ICAO en el DNIe se muestra en la siguiente tabla:

MF			
AID (DF1)			
Data Group	**Nombre EF**	**EF ID**	**Tag**
Común	EF.COM	01 1E	60
DG1	EF.DG1	01 01	61
DG2	EF.DG2	01 02	75
DG3	EF.DG3	01 03	63
DG4	EF.DG4	01 04	76
DG5	EF.DG5	01 05	65
DG6	EF.DG6	01 06	66
DG7	EF.DG7	01 07	67
DG8	EF.DG8	01 08	68
DG9	EF.DG9	01 09	69
DG10	EF.DG10	01 0A	6A
DG11	EF.DG11	01 0B	6B
DG12	EF.DG12	01 0C	6C
DG13	EF.DG13	01 0D	6D
DG14	EF.DG14	01 0E	6E
DG15	EF.DG15	01 0F	6F
DG16	EF.DG16	01 10	70
Objeto de seguridad	$EF.SO_D$	01 1D	77

Grupos de datos y objetos en el contexto LDS

6. Protocolo de comunicación

El protocolo de intercambio de datos utilizado en este documento es el orientado a bloques: T = 1

III. COMANDOS

La siguiente lista, corresponde a los comandos APDU básicos relacionados al sistema de archivos.

CLA	INS	Comando	Descripción
00h | 04h | 0Ch	A4h	Seleccionar contexto	Selecciona la instancia de la aplicación (PKI, ICAO)
00h | 04h | 0Ch	A4h	Seleccionar archivo	Seleccionar el MF, DF, EF o DG
00h | 04h | 0Ch	B0h	Lectura archivo binario	Leer un archivo binario

Comandos APDU relacionados al sistema de archivos

1. Comando Seleccionar contexto

1.1. Descripción

El comando selecciona la instancia de la aplicación que reside en el DNIe y define un contexto PKI o ICAO

1.2. Comando APDU

El mensaje está codificado de acuerdo al formato APDU Nº 3 con la siguiente descripción.

Campo	Valor				Tamaño (bytes)
CLA	00h				1
INS	A4h				1
P1	04h				1
P2	00h	PKI	0Ch	ICAO	1
Lc	10h		07h		1
DATA	AID				16 | 7

Comando Seleccionar Aplicación

Parámetro de Control P1

En ambos contextos, el valor 04h indica la selección de una aplicación.

Parámetro de control P2

En el contexto PKI, el valor 00h indica que un FCI debe ser devuelto por la aplicación, este FCI está contenido en el campo Data del APDU respuesta. En el contexto ICAO, el parámetro toma el valor 0Ch.

Campo DATA

El campo DATA del comando debe contener el AID de la instancia de la aplicación (PKI o LDS).

1.3. Respuesta APDU

El mensaje de respuesta está codificado de acuerdo al formato APDU Nº 5 con la siguiente descripción.

En el contexto ICAO, el campo Data del APDU respuesta es siempre vacío.

En el contexto PKI, el campo Data del APDU respuesta solo está presente si el parámetro de control P2 tiene el valor 00h; en este caso contiene un FCI cuyos bloques TLV se describen a continuación.

T_A	L_A	V_A		
6Fh	X	84h	Y	AID

FCI retornado cuando se selecciona el aplicativo AID

X	Longitud del valor V_A, que corresponde al Tag 6Fh
Y	Longitud del AID seleccionado, que corresponde al Tag 84h

Longitudes presentes en el FCI retornado

1.4. Status Word

SW1 SW2	**Significado**
6E00h	Campo CLA incorrecto
6A82h	AID especificado no existe
6A86h	Combinación (P1,P2) incorrecta
6A87h	Lc inconsistente con (P1,P2): AID varía entre 5 y 16 bytes
6A80h	Datos erróneos en el campo DATA
6700h	Campo Lc incorrecto

Status Word para el comando Seleccionar Aplicación

2. Comando Seleccionar archivo

2.1. Descripción

En el contexto PKI, el comando selecciona los tres tipos de archivos disponibles, MF, DF o EF. La selección de un MF es única; después de una selección satisfactoria de un DF, aquel DF se convierte en el DF actualmente seleccionado o simplemente en el DF actual. Asimismo, el EF actual está configurado a NULL. Los archivos seleccionados previamente no experimentan cambio cuando una selección falla.

En el contexto ICAO, el comando selecciona cualquier archivo DG disponible.

2.2. Comando APDU

El mensaje está codificado de acuerdo al formato APDU Nº 3, con la siguiente descripción.

Campo	Valor				Tamaño (bytes)
CLA	00h				1
INS	A4h				1
P1	00h	PKI	02h	ICAO	1
P2	00h		0Ch		1
Lc	02h - Longitud hexadecimal - campo DATA				1
DATA	EFID				2

Comando Seleccionar Archivo

Parámetro de Control P1

En el contexto PKI, el valor del parámetro de control P1 debe ser 00h, y es utilizado para indicar el modo de selección (implícita) y el tipo de archivo (MF, DF o EF) a ser seleccionado.

En el contexto ICAO, el valor del parámetro debe ser 02h y permite seleccionar un DG disponible.

Parámetro de control P2

El valor del parámetro de control P2 es único y depende del contexto actual.

En el contexto PKI, este es utilizado para indicar que un FCI debe ser devuelto por la aplicación.

Campo DATA

En ambos contextos, el campo DATA debe contener el EFID del archivo a seleccionar.

2.3. Respuesta APDU

Como resultado a la ejecución del comando *Seleccionar Archivo*, el mensaje de respuesta es recibido según el formato APDU Nº 5.

En el contexto ICAO, el campo Data contenido en el APDU respuesta es siempre vacío.

En el contexto PKI, toda la información relevante para el MF, DF o EF está definida en su FCI, este FCI es retornado en el campo Data. La estructura del FCI tiene concordancia con el tipo de archivo seleccionado. El campo Data está codificado mediante una concatenación de tripletes TLV cuyos valores (V) se describen enseguida.

62h	15h	82h	01h	V_A	83h	02h	V_B	85h	02h	V_C	86h	08h	V_D

FCI de un MF

V_A	Descriptor de archivo ‘38’
V_B	Identificador de archivo extendido (EFID = 3F00h)
V_C	Número actual de archivos
V_D	Condiciones de acceso

Campos correspondientes a un FCI de un MF

62h	13h	82h	01h	V_A	83h	02h	V_B	85h	02h	V_C	86h	06h	V_D

FCI de un DF

V_A	Descriptor de archivo ‘38’
V_B	Identificador de archivo extendido (EFID = 5015h)
V_C	Número actual de archivos
V_D	Condiciones de acceso

Campos correspondientes a un FCI de un DF

Los archivos elementales (EF) son almacenados bajo el MF o bajo un DF, y su FCI contiene los TLVs a continuación descritos. Para el caso de un EF seleccionado, el TLV conocido como el Tag 80 (80h, 02h, W) contiene el tamaño del EF.

62h	15h	80h	02h	V_A	82h	01h	V_B	83h	02h	V_C	86h	08h	V_D

FCI de un EF

V_A	Tamaño en bytes del archivo binario
V_B	Descriptor de archivo (‘01’)
V_C	Identificador de archivo extendido (EFID)
V_D	Condiciones de acceso

Campos correspondientes a un FCI de un EF

2.4. Status Word

SW1 SW2	**Significado**
6E00h	Campo CLA incorrecto
6A82h	Archivo especificado no existe
6A86h	Combinación (P1,P2) incorrecta
6A80h	Datos erróneos en el campo DATA
6700h	Campo Lc incorrecto
9000h	Ejecución correcta

Status Word para el comando Seleccionar Archivo

3. Comando de Lectura Binaria

3.1 Descripción

En ambos contextos, el comando es ejecutado sobre el último EF seleccionado. Un EF está conformado por un conjunto de registros de 256 bytes cada uno. La lectura se realiza sobre todos los registros que conforman el EF seleccionado. Estos registros son consecutivos y son indicados por el parámetro P1. El parámetro P2 contiene el offset del registro actual indicado por P1 y debe ser menor al máximo tamaño del registro (256 bytes). Si el tamaño del archivo es nulo y el número de bytes a leer es nulo también el comando retornará un campo Data vacío y un estado 9000h.

3.2 Comando APDU

El mensaje está codificado de acuerdo al formato APDU Nº 2, con la siguiente descripción.

Campo	**Valor**	**Tamaño (bytes)**
CLA	00h o 04h	1
INS	B0h	1
P1	ID del registro contenido en el EF en hexadecimal	1
P2	00h	1
Le	00h - significa 256 bytes Número de bytes del registro a leer (menor a 256 bytes)	1

Comando de Lectura Binaria

Parámetro de Control P1

Contiene el ID del registro a leer perteneciente a un EF actual. En el caso de EFs cuyos tamaños indicados por el Tag 80 son mayores a 256 bytes, el ID del primer registro es 00h y el ID del último registro para el EF actual se obtiene calculando el cociente del valor del Tag 80 y 256.

Parámetro de control P2

El parámetro P2 indica el offset del registro actual. El offset es el primer byte desde donde se leen los datos del registro actual indicado por P1, el valor 00h indica que la lectura se realiza en el inicio del registro.

Parámetro Le

Contiene el número de bytes a ser leídos en el registro indicado por P1, y que se espera en el campo Data de la respuesta correspondiente, el valor 00h indica que se lee todo el registro, o sea 256 bytes; para el caso del último registro del EF actual el valor del parámetro en bytes se obtiene calculando el resto del valor del Tag 80 y 256.

3.3 Respuesta APDU

Como resultado a la ejecución del comando *Lectura de Archivo Binario*, el mensaje de respuesta es recibido según el formato APDU Nº 5.

A menos de que el comando falle, el campo Data de la respuesta contiene el número de bytes requeridos leídos desde la última combinación (P1, P2) especificada.

3.4 Status Word

SW1 SW2	**Significado**
6282h	La longitud de los datos restantes son menores que los datos esperados
6700h	Campo Lc incorrecto
6E00h	Campo CLA incorrecto
6986h	No es el actual EF
6981h	El actual EF no es un archivo binario
6982h	Estado de seguridad insatisfecho
6A80h	Campo DATA erróneo
6A82h	EFID inválido
6A86h	P1 incorrecto (bit 8 debe ser 0)
6B00h	Offset incorrecto del primer byte a ser leído
6CLLh	Le inválido (no más de LL bytes pueden ser leídos desde el offset especificado)
6281h	Sin datos, el tamaño del archivo es cero
9000h	Ejecución correcta

Status Word para el comando de Lectura Binaria

La siguiente lista, corresponde a los comandos APDU básicos relacionados a las credenciales.

CLA	**INS**	**Comando**	**Descripción**
00h o 04h	20h	Verificar PIN	Verificar la credencial (PIN) del DNIe
00h o 04h	21h	Verificación Biométrica	Verificación de identidad biométrica del Titular del DNIe

Comandos APDU relacionados a las credenciales

4. Comando Verificar PIN

4.1 Descripción

El comando es usado en modo plano o dentro de un canal seguro SMA. Después de una verificación satisfactoria del PIN el contador de número de intentos asociado es reiniciado a su máximo valor y los derechos de acceso asociados quedan garantizados. Estos derechos de acceso permanecen válidos hasta que una re-selección de la aplicación o un apagado ocurran.

Si la verificación falla debido a que el PIN suministrado es erróneo, el contador de número de intentos experimenta un decremento en 1, y si el contador llega a cero, la credencial es bloqueada. Si la credencial es bloqueada, ninguna otra verificación puede ser procesada, aún con el PIN correcto.

4.2 Comando APDU

El mensaje está codificado de acuerdo al formato APDU Nº 3, con la siguiente descripción.

Campo	Valor	Tamaño (bytes)
CLA	00h o 04h	1
INS	20h	1
P1	00h	1
P2	ID de la credencial en hexadecimal	1
Lc	08h - Longitud hexadecimal - campo DATA	1
DATA	PIN candidato en hexadecimal	8

Comando Verificar PIN

Parámetro de Control P1

El valor del parámetro de control P1 debe ser 00h.

Parámetro de Control P2

El valor del parámetro de control P2 identifica el ID de la credencial a ser verificada o invalidada.

Valor	Significado
01h	Referencia a la credencial de Autenticación
04h	Referencia a la credencial de Firma

ID de la credencial

Campo DATA

El campo DATA permite introducir un PIN de 8 dígitos como máximo y todos ellos deben estar presentes.

Los dígitos deben ingresarse de forma consecutiva hasta completar los 8 dígitos disponibles. Si el contenido del PIN es menor que los 8 dígitos disponibles, los dígitos restantes no utilizados se rellenan con el valor FFh.

4.3 Respuesta APDU

Como resultado a la ejecución del comando *Verificar PIN*, el mensaje de respuesta es recibido según el formato APDU Nº 5. El campo Data de la respuesta se encuentra vacío.

4.4 Status Word

SW1 SW2	Significado
63Cxh	Comparación fallida; se dispone de (x) intentos
6984h	Data referenciada no fue inicializada
6983h	El límite de intentos es superado o la credencial está bloqueada
6A86h	Parámetro P1 y/o P2 incorrectos
6A88h	La credencial no existe o es incompatible con el comando
9000h	Ejecución normal

Status Word para el comando Verificar PIN

5. Comando Verificación Biométrica

5.1 Descripción

Este comando puede ser utilizado en modo plano o dentro de un canal seguro SMA. Después de una verificación satisfactoria de esta credencial, el contador de intentos asociado a esta credencial es establecido a su valor máximo y los derechos de acceso asociados con esta credencial son garantizados.

Estos derechos de acceso permanecen válidos hasta que un nuevo comando de verificación falle y lo invalide, o la sesión del DNIe sea reiniciada.

Así también, el valor de este contador disminuye cuando la verificación falla, y la credencial pasa al estado bloqueado cuando el contador alcanza la cantidad de cero re-intentos.

5.2 Comando APDU

El comando está codificado de acuerdo al formato APDU Nº 3, con la siguiente descripción:

Campo	**Valor**	**Tamaño (bytes)**
CLA	00h o 04h	1
INS	21h	1
P1	00h	1
P2	00h	1
Lc	Longitud hexadecimal del campo DATA	1
DATA	Plantilla de Datos biométrico en hexadecimal	variable

Comando Verificación Biométrica

Parámetros de control (P1, P2)

La combinación de valores (00h, 00h) designan la operación de Verificación Biométrica.

Campo DATA

El campo DATA es especificado de la siguiente forma:

T_1	**L_1**	**V_1**		
7Fh		**T_2**	**L_2**	**V_2**
2Eh	N	X	Número de bytes en hexadecimal de V_2	Plantilla Biométrica ISO/IEC 19794-2

Estructura del campo DATA del comando Verificación Biométrica

Campo	**Condición**	**Valor del Campo**	**Tamaño (bytes)**
Etiqueta **X**	L_2+1 < 128 bytes	81h	1
	Otro caso	8181h	2
Longitud **N**	L_1 < 128 bytes	L_1h	1
	Otro caso	81L_1h	2

Valores de los campos contenidos en el campo DATA del comando Verificación Biométrica

5.3 Respuesta APDU

Como resultado a la ejecución del comando *Verificación Biométrica*, el mensaje de respuesta es recibido según el formato APDU Nº 5. El campo Data de la respuesta se encuentra vacío.

5.4 Status Word

SW1 SW2	Significado
6A88h	La plantilla biométrica no existe
6983h	La plantilla biométrica fue bloqueada antes del intento de verificación
6986h	Comando no permitido
6A80h	Formato de datos inválido
63Cxh	Datos biométricos incorrectos, el número de intentos restantes es x
9000h	Ejecución exitosa

Status Word para el comando Verificación Biométrica

La siguiente lista, corresponde a los comandos APDU básicos relacionados a mecanismos criptográficos.

CLA	INS	Comando	Descripción
00h o 04h	22h	MSE - set	Manage Security Environment - set
10h o 00h	2Ah	PSO	Performance Security Operation

Comandos APDU relacionados a mecanismos criptográficos

6. Comando MSE – set

6.1 Descripción

El comando es utilizado para configurar los parámetros de un CRT, paso necesario previo a la ejecución de una operación criptográfica. Todas los CRDOs son volátiles y deben estar definidos antes de la ejecución de cualquier comando PSO.

6.2 Comando APDU

El mensaje está codificado de acuerdo al formato APDU Nº 3, con la siguiente descripción.

Campo	Valor	Tamaño (bytes)
CLA	00h o 04h	1
INS	22h	1
P1	41h (SET)	1
P2	B6h (CRT)	1
Lc	06h (Longitud hexadecimal del campo DATA)	1
DATA	CRDO relevante para la operación específica y CRT	6

Comando MSE - set

Parámetro de Control P1

El valor del parámetro de control P1 debe ser 41h; y designa la operación criptográfica (SET) para el cual, el CRDO transmitido es válido.

Parámetro de Control P2

El valor del parámetro de control P2 designa el CRT a ser colocado. El valor de B6h indica que el CRT utilizado es el (Digital Signature Template) y este debe ser establecido previo a la ejecución del comando PSO.

Campo DATA

El campo DATA contiene uno o más CRDOs (TLVs concatenados). El Tag y la Longitud del CRT coinciden con los valores de P2 y Lc, por tanto, no son transmitidos. El CRDO transmitido depende del CRT a ser inicializado, y para el caso del CRT con valor B6h, los siguientes DO son incorporados.

P2	Lc	DATA					
B6h	06h	80h	01h	V_A	83h	01h	V_B

CRDOs incluidos en el CRT para el comando MSE - set

El Tag 80h hace referencia al mecanismo criptográfico a utilizar (Identificador del algoritmo). El Tag 83h es usado para designar la clave (secreta) a ser usada por las siguientes operaciones criptográficas (ID de referencia a la clave privada)

Valor V_A	Significado
11h	RSA con mecanismo PKCS#1

Identificador de algoritmo para las claves

Valor V_B	Significado
01h	Referencia a la clave privada de Autenticación
02h	Referencia a la clave privada de Firma

Identificador de la clave privada

6.3 Respuesta APDU

Como resultado a la ejecución del comando *MSE - set*, el mensaje de respuesta es recibido según el formato APDU Nº 5. El campo Data de la respuesta se encuentra vacío.

6.4 Status Word

SW1 SW2	**Significado**
6A80h	Tag inválido o ausente, longitud o valor en un CRDO
6A88h	El objeto criptográfico referenciado no existe
6982h	El parámetro de control de seguridad no fue satisfactorio
6A86h	Parámetro P1 y/o P2 incorrectos
6981h	El tipo de clave seleccionada o especificada es inconsistente con el mecanismo
6600h	El entorno de seguridad no puede ser configurado
9000h	Ejecución correcta

Status Word para el comando MSE – set

7. Comando PSO

7.1 Descripción

El comando PSO inicia las operaciones de seguridad de acuerdo a la combinación (P1, P2) seleccionada.

7.2 Comando APDU

El mensaje está codificado de acuerdo al formato APDU Nº 3, con la siguiente descripción.

Campo	**Valor**	**Tamaño (bytes)**
CLA	10h o 00h	1
INS	2Ah	1
P1	9Eh	1
P2	9Ah	1
Lc	Longitud hexadecimal del campo DATA	1
DATA	Representación de los datos a ser firmados	variable

Comando PSO

Parámetros de control (P1, P2)

La combinación de valores (9Eh, 9Ah) designan la operación de seguridad de Firma digital.

Campo DATA

El campo DATA está conformado por la concatenación del OID del algoritmo de Hash utilizado, y el Hash del dato que se desea firmar. Esta concatenación es descrita a continuación.

T	L	V					
30h	L	30h	L_A	V_A	04h	L_B	V_B

Campo DATA para la operación de Firma digital

Para el TLV representado por el triplete (30h, L_A, V_A). El valor de V_A contiene los índices hexadecimales del Hash utilizado. El valor de L_A representa la longitud de estos índices.

Para el TLV representado por el triplete (04h, L_B, V_B). El valor de V_B contiene el hash correspondiente del dato a firmar. El valor de L_B representa la longitud de este hash.

Para el TLV representado por el triplete (30h, L, V). V representa la concatenación de los TLVs antes descritos. El valor de L se obtiene con la siguiente fórmula aritmética.

$$L = L_A + 02h + L_B + 02h$$

Valor de L para el triplete contenido en el campo DATA

Nota: Los algoritmos de Hash contemplados en este documento son: SHA 1 y SHA 256.

7.3 Respuesta APDU

Como resultado a la ejecución del comando *PSO*, el mensaje de respuesta es recibido según el formato APDU Nº 5.

El campo Data de la respuesta contiene la firma del Hash del dato suministrado.

7.4 Status Word

SW1 SW2	**Significado**
6985h	El comando MSE-set precedente no se ha ejecutado o el archivo de la clave especificada previamente ha sido borrado.
6985h	El contador de uso de la clave ha sido superado o las condiciones de accesos no se satisfacen.
6700h	La longitud de los datos es errada
6A80h	El mecanismo es incompatible
6A86h	Combinación (P1, P2) incorrecta

Status Word para el comando PSO

La siguiente lista, corresponde a los comandos APDU relacionados a la creación de una canal seguro SMA.

CLA	**INS**	**Comando**	**Descripción**
80h	46h	Generar par de claves SMA	Genera el par de claves RSA utilizadas para establecer la sesión SMA
00h	84h	Obtener desafío	Obtiene el mensaje de control y la clave maestra (semillas)
00h	86h	Autenticación General	Envía al DNIe el bloque PKCS#1 tipo 2 cifrado para obtener las claves de sesión SMA.

Comandos APDU relacionados a la creación de una canal seguro SMA en el contexto PKI

8. Generar par de claves SMA

8.1 Descripción

Para establecer una sesión de canal seguro SMA, se requiere implementar un protocolo de intercambio de claves. El protocolo requiere de la generación de un par de claves RSA, que serán utilizadas para cifrar el intercambio de elementos requeridos en el establecimiento del canal seguro entre el terminal y el DNIe.

8.2 Comando APDU

El mensaje está codificado, de acuerdo al formato APDU Nº 4, con la siguiente descripción.

Campo	Valor	Tamaño (bytes)
CLA	80h	1
INS	46h	1
P1	00h	1
P2	00h	1
Lc	04h	1
DATA	A0020400h (1024 bits)	4
Le	8Ch (Longitud clave pública retornada)	140

Comando Generar par de claves SMA

8.3 Respuesta APDU

El mensaje está codificado, de acuerdo al formato APDU Nº 5. La generación del par de claves RSA retorna la clave pública del par generado contenido en el campo Data del APDU respuesta.

La clave privada reside en el DNIe mientras la sesión no termine.

8.4 Status Word

SW1 SW2	Significado
6A86h	Combinación (P1,P2) incorrecto
6A80h	Campo DATA incorrecto

Status Word para el comando Generar Par de Claves SMA

9. Obtener desafío

9.1 Descripción

En el contexto PKI, la instrucción obtener desafío, es usada para autenticar una credencial o iniciar el establecimiento de un canal seguro SMA. Ésta genera y retorna una cadena aleatoria con una longitud de 24 bytes. En el contexto ICAO, la instrucción es utilizada para generar una cadena aleatoria de 8 bytes desde el DNIe y se emplea en el establecimiento de un BAC.

9.2 Comando APDU

El mensaje está codificado, de acuerdo al formato APDU Nº 2, con la siguiente descripción.

Campo	Valor		Tamaño (bytes)
CLA	00h		1
INS	84h		1
P1	00h		1
P2	00h		1
Le	00h (24 bytes) - PKI	08h - ICAO	1

Comando Obtener desafío

9.3 Respuesta APDU

En el contexto ICAO, el campo Data del APDU respuesta contiene el desafío generado de 8 bytes.

En el contexto PKI, para la autenticación de una credencial, el campo Data representa una cadena aleatoria. Para el establecimiento de un canal seguro SMA.

El campo Data de la respuesta contiene los parámetros RC1 (mensaje de control) y RC2 (clave maestra) como se muestra a continuación.

RC1 (8 bytes)	RC2 (16 bytes)

Campo Data de la respuesta del comando Obtener desafío en el contexto PKI

9.4 Status Word

SW1 SW2	**Significado**
6E00h	Campo CLA incorrecto
6C24h	Campo Le incorrecto
6A86h	P1/P2 incorrecto
9000h	Desafío retornado exitosamente

Status Word para el comando Obtener desafío

10. Autenticación General

10.1 Descripción

Durante el protocolo de intercambio de claves para la creación de un canal seguro SMA, el comando envía un bloque cifrado con la clave pública SMA. Este bloque está empaquetado según las reglas del formato PKCS#1, tipo 2.

El empaquetado contiene la clave de encriptación ENC y la clave MAC de la pre-sesión, y el mensaje de control RC1. El comando descifra el bloque enviado, y verifica el valor del mensaje de control RC1.

A continuación, calcula la clave de encriptación ENC y la clave MAC de la sesión, y se conservan en el DNIe durante la sesión.

10.2 Comando APDU

El mensaje está codificado, de acuerdo al formato APDU Nº 3, con la siguiente descripción.

Campo	**Valor**	**Tamaño (bytes)**
CLA	00h	1
INS	86h	1
P1	08h	1
P2	00h	1
Lc	80h (Longitud del campo cifrado DATA)	1
DATA	Bloque PKCS#1 Tipo 2 cifrado con la clave pública SMA	128

Comando Autenticación General

Parámetros de control (P1, P2)

La combinación de parámetros (P1, P2) es única, y se muestra en la tabla anterior.

Campo DATA

El campo DATA es la construcción del bloque PKCS#1 Tipo 2 cifrado con la clave pública SMA.

10.3 Respuesta APDU

El mensaje de respuesta está codificado de acuerdo al formato APDU Nº 5 con la siguiente descripción.

El contenido del campo Data del APDU respuesta retorna una cadena de 17 bytes que contiene la concatenación del ID de la sesión y el R-MAC (utilizado en la creación del MAC del comando), ordenados de la siguiente manera:

ID de la sesión (01 byte)	R-MAC (16 bytes)

Campo Data de la respuesta del comando Autenticación General

10.4 Status Word

SW1 SW2	**Significado**
6A86h	Combinación (P1,P2) incorrecta
6A80h	Campo DATA incorrecto

Status Word para el comando Autenticación General

La siguiente lista, corresponde a los comandos APDU relacionados a la aplicación LDS.

CLA	**INS**	**Comando**	**Descripción**
00h	88h	Autenticación interna	Realizar autenticación activa
00h	82h	Autenticación externa	Realizar un BAC

Comandos APDU relacionados a la lectura de datos del ciudadano en el contexto ICAO

11. Autenticación Interna

11.1 Descripción

El comando es usado para realizar una autenticación activa.

Los pasos a realizar para efectuar una autenticación activa y sus requerimientos están especificados en la Norma ICAO.

11.2 Comando APDU

El mensaje está codificado de acuerdo al formato APDU Nº 4 con la siguiente descripción.

Campo	**Valor**	**Tamaño (bytes)**
CLA	00h	1
INS	88h	1
P1	00h	1
P2	00h	1
Lc	08h	1
DATA	Cadena aleatoria desde el Host	8
Le	Longitud esperada de la respuesta	1

Comando Autenticación Interna

Parámetros de control (P1, P2)

La combinación de parámetros (P1, P2) es única, sus valores se muestran en la tabla anterior.

Campo DATA

El campo DATA del comando enviado contendrá 8 bytes aleatorios desde el sistema de inspección.

11.3 Respuesta APDU

El mensaje está codificado, de acuerdo al formato APDU Nº 5 con la siguiente descripción.

El campo data contenido en el APDU respuesta contiene la firma *S* descrita en la norma ICAO, calculada internamente en el DNIe.

11.4 Status Word

SW1 SW2	Significado
6D00h	INS incorrecto, autenticación activa, no soportada
6E00h	CLA incorrecto
6A86h	P1/P2 incorrecto
6700h	Lc incorrecto, se espera 8 bytes
6A81h	El comando no puede ser procesado, algunas características criptográficas no están presentes
9000h	Ejecución correcta

Status Word para el comando Autenticación Interna

12. Autenticación Externa

12.1 Descripción

El comando es usado para realizar un BAC. El procedimiento está especificado en la norma ICAO.

12.2 Comando APDU

El mensaje está codificado de acuerdo al formato APDU Nº 4 con la siguiente descripción.

Campo	Valor	Tamaño (bytes)
CLA	00h	1
INS	82h	1
P1	00h	1
P2	00h	1
Lc	28h - Longitud del campo DATA	1
DATA	Cadena cifrada de entrada	40
Le	28h - Longitud esperada en la respuesta	1

Comando Autenticación Externa

Parámetros de control (P1, P2)

La combinación de parámetros (P1, P2) es única, sus valores se muestran en la tabla anterior.

Campo DATA

El campo DATA del comando enviado contiene la cadena cifrada externa calculada por la aplicación, que tiene que ser verificada. Si un BAC se está realizando, la longitud de la data enviada es de 40 bytes.

12.3 Respuesta APDU

El mensaje está codificado, de acuerdo al formato APDU Nº 5 con la siguiente descripción.

El campo data contenido en el APDU respuesta contiene una cadena cifrada de 40 bytes de longitud, si un BAC se está realizando.

12.4 Status Word

SW1 SW2	**Significado**
6D00h	INS incorrecto, característica BAC no soportada
6985h	Secuencia errónea
6E00h	CLA incorrecto
6A86h	Combinación (P1,P2) incorrecta
6700h	Lc incorrecto
6A80h	Data errónea
6300h	Autenticación BAC errónea
9000h	Ejecución correcta

Status Word para el comando Autenticación Externa

IV. Estructura del Registro ABI

El campo Data del APDU respuesta a la lectura del EF *FD01* contiene los datos del registro ABI del DNIe. La cadena hexadecimal obtenida en el campo Data del APDU respuesta está organizada en objetos TLV según la siguiente estructura:

Campo Data:

T	**L**	**V**	
78h	Longitud total (variable)	TLV_A	TLV_B

TLV del Campo Data de la respuesta a la lectura del registro ABI

El TLV_A tiene los siguientes campos:

T_A	**L_A**	**V_A**
5Ch	18h	V_A

Primera trama TLV contenida en el campo Valor de la respuesta a la lectura del registro ABI

El valor del campo V_A:

5F60h	5F61h	5F62h	5F63h	5F64h	5F6Ah	5F21h	5F22h	5F23h	5F7Dh	5F7Bh	5F7Ch

Campo Valor de la primera trama TLV contenida en el campo Valor de la respuesta a la lectura del registro

El campo TLV_B es la concatenación de los siguientes TLVs listados a continuación:

T_B	**L_B**	**V_B**
5F60h	08h	Valor CUI
5F61h	01h	Valor Dígito de verificación
5F62h	Longitud Primer Apellido	Valor Primer Apellido
5F63h	Longitud Segundo Apellido	Valor Segundo Apellido
5F64h	Longitud Pre Nombres	Valor Pre Nombres
5F6Ah	01h	Valor Género (46h o 4Fh)
5F21h	06h	Valor Ubigeo
5F22h	06h	Valor Grupo de Votación
5F23h	04h	Valor
5F7Dh	00h	-
5F7Bh	00h	-
5F7Ch	04h	Valor

Objetos TLV contenidos en la segunda trama del campo Valor de la respuesta a la lectura del registro ABI

La longitud completa del APDU respuesta a la lectura de los datos ABI es de 256 bytes. Los datos ABI no exceden este tamaño.

V. Referencias:

I. ISO/IEC 7816-4:2013 : Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange

II. ISO/IEC 7816-3:2006 : Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols

III. ICAO Doc 9303:2008 : Machine Readable Travel Documents - Part 3: Machine Readable Official Travel Documents, Vol 2: Specifications for electronically enabled official travel documents with biometric identification capability