Guía de uso de CI electrónica a través de APDU

Imprimir

Table of Contents [-]

6. Validación de la huella digital de la persona Match On Card (https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Gu%C3%ADa+de+uso+de+CI+electr%C3%B3nica+a+trav%C3%A9s+de+APDU/pop_up#section-Guía+de+uso+de+CI+electrónica+a+través+de+APDU-Validación+de+la+huella+digital+de+la+persona+Match+On+Card)
7. Extracción de los datos de identificación de la persona (https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Gu%C3%ADa+de+uso+de+CI+electr%C3%B3nica+a+trav%C3%A9s+de+APDU/pop_up#section-Guía+de+uso+de+CI+electrónica+a+través+de+APDU-Extracción+de+los+datos+de+identificación+de+la+persona)
8. Firma Digital (https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Gu%C3%ADa+de+uso+de+CI+electr%C3%B3nica+a+trav%C3%A9s+de+APDU/pop_up#section-Guía+de+uso+de+CI+electrónica+a+través+de+APDU-Firma+Digital)
    1. Ejemplo de firma digital (https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Gu%C3%ADa+de+uso+de+CI+electr%C3%B3nica+a+trav%C3%A9s+de+APDU/pop_up#section-Guía+de+uso+de+CI+electrónica+a+través+de+APDU-Ejemplo+de+firma+digital)
    2. Repositorios públicos de ejemplo (https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Gu%C3%ADa+de+uso+de+CI+electr%C3%B3nica+a+trav%C3%A9s+de+APDU/pop_up#section-Guía+de+uso+de+CI+electrónica+a+través+de+APDU-Repositorios+públicos+de+ejemplo)

¿Qué es un APDU y por qué es relevante?

El Application Protocol Data Unit (APDU) es la unidad de comunicación entre un lector de tarjetas inteligentes y una tarjeta inteligente, en inglés *Smart Card*. Dado que la Cédula de Identidad Electrónica es en esencia una Smart Card conformante con el estándar ISO 7816, esta es la unidad lógica utilizada para comunicarse con la misma a bajo nivel.

Si bien existen otras vías para comunicarse con la CI Electrónica, como drivers PKCS#11, plug-ins, bibliotecas, etc., todas estas vías se implementan utilizando APDU, es decir, son *wrappers*. Poder interactuar con las aplicaciones de la CI Electrónica a través de APDU tiene la ventaja de que otorga la máxima flexibilidad a nivel de plataformas en las que se puede implementar la interacción, y además, hay operaciones como el *Match On Card (MOC)* para las que no se cuenta con una biblioteca de más alto nivel, por lo que **sólo pueden realizarse a través de esta vía**.

Estructura de un APDU

Hay dos tipos de APDUs: comandos y respuestas. Los comandos APDU los envía el lector a la tarjeta, las respuesta APDU las envía la tarjeta al lector.

La estructura de un APDU está definida en los estándares ISO/IEC 7816.

Estructura de un comando APDU

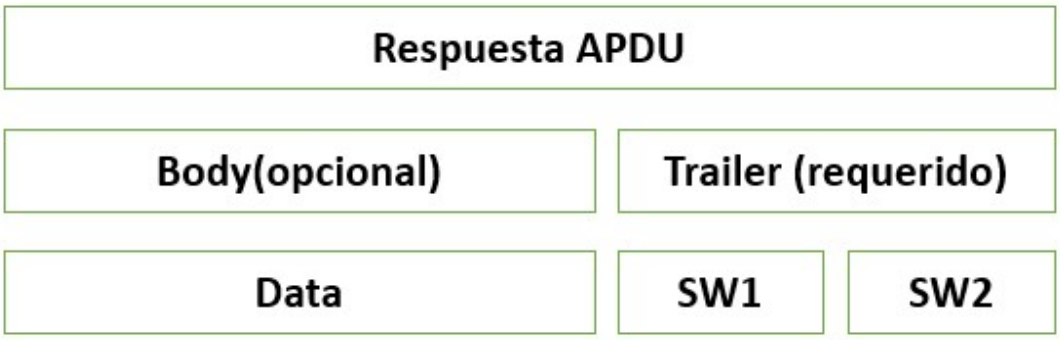
La trama APDU de tipo comando consta de los siguientes campos:

- **CLA :** Byte de clase
- **INS :** Byte de instrucción
- **P1,P2:** Parámetros
- **Lc :** tamaño del bloque de datos
- **Data**
- **Le :** Tamaño de la respuesta esperada

Los 4 primeros son obligatorios, mientras que los relacionados con los datos y la respuesta esperada son opcionales. A partir del byte de instrucción, la tarjeta sabe qué es lo que se le pide.

Contienen una cabecera obligatoria de 4/5 bytes, y entre 0 y 255 bytes de datos.

Estructura de una respuesta APDU



La trama APDU respuesta consta de los campos:

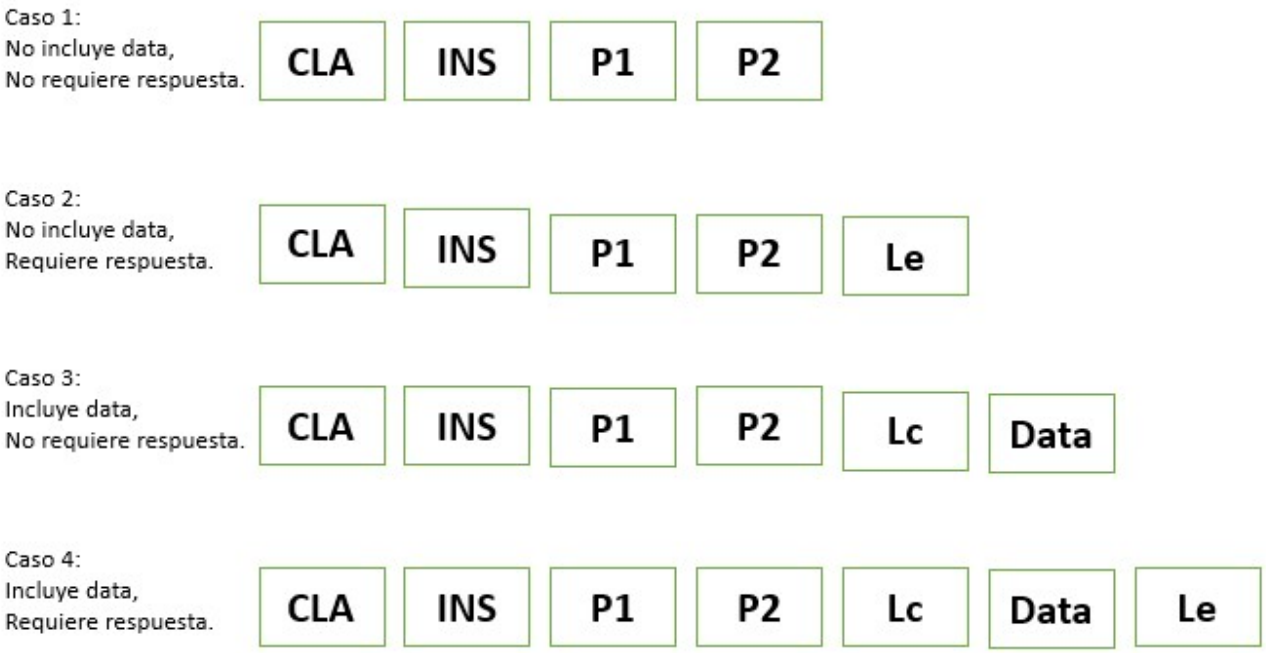
- **Data**
- **SW1, SW2:** Palabra de estado, dónde se codifica el estado de la operación (correcta, error criptográfico, error general...). Una vez más, los datos son opcionales pero el código de estado es obligatorio.

Contienen una palabra de estado obligatoria de 2 bytes, y entre 0 y 255 bytes de datos.

Casos de APDU

Existen 4 casos definidos para comandos APDU donde la estructura varia de la siguiente forma:

1. El largo Lc es nulo; por lo tanto los campos Lc y data van vacíos. El largo Le es también nulo; por lo tanto el campo Le va vacío. Por consecuencia, el campo Body es vacío.
2. El largo Lc es nulo; por lo tanto los campos Lc y data van vacíos. El largo Le no es nulo; por lo tanto el campo Le está presente. Por consecuencia, el campo Body es el Le.
3. El largo Lc no es nulo; por lo tanto el campo Lc está presente y define el largo de campo Data también presente. El largo Le es nulo; por lo tanto el campo Le es vacío. Por consecuencia, el Body contiene al campo Lc seguido del campo data.
4. El largo Lc no es nulo; por lo tanto el campo Lc está presente y define el largo del campo Data también presente. El largo Le no es nulo; por lo tanto el campo Le esta presente. Por consecuencia, el Body consiste en el campo Lc seguido del campo Data seguido del campo Le.



Formato TLV para datos

Para ciertos tipos de operaciones, la información dentro del campo Data en los comandos y respuestas APDU está representada en formato TLV "Tag Length Value" (Tipo Longitud Valor).

Este formato permite organizar mejor la información y tiene la siguiente lógica:

- **TAG:** Representa la información contenida en el campo VALUE.
- **LENGTH:** Largo en bytes de la información contenida en el campo VALUE.
- **VALUE:** Información.

Ejemplo de un TLV que contiene el número de documento de la persona obtenido como parte del caso de uso de extracción de los datos de identificación:

Como se ve en el ejemplo el TAG 5F01 representa al Número de documento que tiene largo en bytes 09.

El campo LENGTH viene habitualmente en un byte, pero cuando el tamaño del VALUE es mayor a 0x7F (127), en el campo LENGTH el primer bit será 1 y los restantes indican el tamaño en bytes restantes del campo. Esto se traduce a que será 0x80 + tamaño restante de LENGTH. Entonces:

Si 0 <= LENGTH < 0x7F(127) => LENGTH 1 byte = XX

Si 0x7F < LENGTH < 0xFF(255) => LENGTH 2 byte = 81 XX

Si 0xFF < LENGTH < 0xFFFF(65535) => LENGTH 3 byte = 82 XX XX

etc

Por ejemplo en el caso de obtener la imagen de la persona el campo LENGTH contendrá un byte con el número 0x82 seguido del largo representado en 2 bytes, por ejemplo T= 0x3F01 L= 0x8223FE D= 9214 bytes(0x23FE). También ocurre esto cuando se envían 42 o más minucias al match on card.

Comandos APDU y Casos de uso

En esta sección se presentan los comandos APDU que luego serán utilizados en conjunto para la construcción de casos de uso como por ejemplo extraer los datos de identificación del documento.

Selección del Applet de firma IAS - selectIAS

El comando select selecciona el Applet IAS de firma por su AID (Application Identifier) dentro del eID.

Es precondición para cualquier otro comando APDU descripto en este documento que se haga un select del Applet IAS antes.

La estructura de un comando de selección de aplicación por su AID es la siguiente:

	CLA	INS	P1	P2	Lc	Data
Caso 3: Incluye data, No requiere respuesta.	**00**	**A4**	**04**	**00**	**Lc**	**AID**

El comando APDU que selecciona el applet de firma IAS:

CLA	INS	P1	P2	Lc	Data
00	**A4**	**04**	**00**	**0C**	**A0 00 00 00 18 40 00 00 01 63 42 00 00**

IMPORTANTE: El comando selectIAS se debe ejecutar al inicio antes que cualquier otro comando

Seleccion de un archivo por el ID de archivo - selectFile

La información contenida en el eID como por ejemplo los datos de identificacion o certificado de la persona se encuentra distribuida en archivos y cada archivo se identifica por un ID.

Para realizar la lectura de esta información se debe seleccionar el archivo por su correspondiente ID utilizando el comando APDU *selectFile*.

Luego de realizada la selección del archivo mediante su ID, el comando APDU *readBinary* se envía para extraer los datos. Para el envío del comando *readBinary* se debe conocer el tamaño del archivo a leer.

Este dato necesario para la lectura del archivo se encuentra en lo que se denomina FCI Template. El FCI Template de cada archivo se obtiene de la respuesta APDU al comando *selectFile*.

Por ejemplo, para leer los datos del certificado del usuario debemos seleccionar primero el archivo correspondiente y obtener su FCI Template.

El FCI Template contiene los siguientes datos de relevancia entre otros:

- Nombre del archivo
- Tamaño del archivo

El tamaño del archivo es necesario para realizar la lectura de la información utilizando el comando *readBinary*.

Entonces, si se quisieran leer los datos del certificado electrónico contenido en el eID se deben realizar los siguientes pasos:

1) Obtener el archivo FCI Template del certificado a través de su ID y la operación *selectFile*.

2) Extraer del FCI Template obtenido en el comando APDU respuesta al comando *selectFile* el tamaño en bytes del certificado.

3) Conociendo el tamaño del archivo que contiene el certificado se ejecuta el comando APDU *readBinary* para obtener la información del certificado.

Estructura del comando *selectFile*:

	CLA	INS	P1	P2	Lc	Data	Le
Caso 4: Incluye data, Requiere respuesta.	**00**	**A4**	**00**	**00**	**02**	**FileID**	**Le**

Ejemplo de un comando de *selectFile* para seleccionar el FCI Template del certificado.

CLA	INS	P1	P2	Lc	Data	Le
00	**A4**	**00**	**00**	**02**	**B0 01**	**Le**

En la respuesta viene el archivo FCI Template correspondiente al certificado. El ID del archivo que contiene al certificado es **"B001"** como se ve en el ejemplo.

0	6Fh	Tag del FCI Template
1	L	Largo de FCI Data
2	81h	Tag de largo de archivo
3	02h	Largo del tamaño del archivo
4–5	Tamaño de archivo	Valor del tamaño del archivo
6	82h	FDB Tag
7	01h	Largo del FDB
8	FDB	Valor del FDB
9	83h	Tag del ID de archivo
10	02h	Largo del archivo ID
11–12	ID Archivo	Valor del ID archivo
13	8Ah	Tag de “Life Cycle Status byte for file"
14	01h	Largo de “Life Cycle Status byte for file”
15	Var.	Valor de “Life Cycle Status byte for file”
16	8Ch	Tag de atributos de seguridad
17	L	Largo de atributos de seguridad
18	AMB	Modo acceso a bytes
19–(18+X)	SCBs	Condición de seguridad bytes (X)

Como se ve en la imagen, el FCI template contiene el tamaño del archivo a leer (offset 4-5), necesario y suficiente para la lectura del mismo.

Lectura de un binario - readBinary

La lectura de un binario se realiza sobre un archivo previamente seleccionado con el comando APDU *selectFile*.

Cada comando *readBinary* puede leer como máximo 0xFF bytes de un archivo, si el tamaño del archivo es superior a 0xFF se deberán enviar tantos comandos APDU *readBinary* como sean necesarios.

Por ejemplo, si el tamaño del certificado a leer (obtenido del FCI Template del archivo) es de 3000 bytes, se deberán enviar 3000/255 + 1 comandos de *readBinary* para completar la lectura del certificado. En este caso 12.

Estructura del comando *readBinary*:

	CLA	INS	P1	P2	Le
Caso 2: No Incluye data, Requiere respuesta.	**00**	**B0**	**P1**	**P2**	**Le**

Donde P1 P2 es el offset en hexadecimal donde empezar a leer datos.

Ejemplo de un comando *readBinary* obteniendo los primeros 255 bytes (0xFF) del archivo seleccionado:

CLA	INS	P1	P2	Le
00	B0	00	00	FF

Para los siguientes READ_BINARY se debe sumar 0xFF al offset y continuar leyendo datos, por ejemplo si L es el largo del archivo en hexadecimal:

00 B0 00 FF Le=FF

00 B0 01 FE Le= FF

00 B0 02 FD Le=FF

.

.

.

00 B01 L1 L2 Le=L3

Donde:

L1 || L2 = 0xFF x cociente(L/0xFF)

L3 = resto(L/0xFF)

Verificación de PIN - verifyPIN

La operación de verificación de PIN es requisito previo a las operaciones de firma.

	CLA	INS	P1	P2	Lc	Data
Caso 3: Incluye data, No requiere respuesta.	CLA	20	00	P2	Lc	Pin de Verificación

- **CLA:**
  - 00h Transmisión en plano
  - 0Ch Transmisión sobre canal seguro
- **INS:**
  - 20h Fijo para la operación de verificación.
- **P1:**
  - 00h Modo verificación
- **P2:**
  - 11h Para global PIN
- **Lc:**
  - 0Ch Siempre espera 12 bytes de largo, se agregan 0's al final como padding.
- **Data:**
  - El PIN va en codificado en ASCII y largo 12 bytes.

Ejemplo de un comando APDU para verificar el PIN 1234:

CLA	INS	P1	P2	Lc	Data
00	20	00	11	0C	31 32 33 34 00 00 00 00 00 00 00 00

Validar PIN verificado - isVerifiedPIN

Valida si el PIN se encuentra verificado.

Caso 1:
No Incluye data,
No requiere respuesta.

CLA	INS	P1	P2	Le
CLA	20	00	P2	00

- **CLA:**
  - 00h Transmisión en plano
  - 0Ch Transmisión sobre canal seguro
- **INS:**
  - 20h Fijo para la operación de verificación.
- **P1:**
  - 00h Modo verificación
- **P2:**
  - 11h Para global PIN
- **Le:**
  - 00h No espera respuesta pero se debe enviar Le o Lc con 00h.
- **Data:**
  - Ausente.

Ejemplo de un comando APDU para verificar si el PIN se encuentra verificado:

CLA	INS	P1	P2	Le
00	20	00	11	00

Validación de la huella digital de la persona Match On Card

Realiza la operación de *Match On Card*. Validación 1 a n comparando las minucias extraídas por un lector de huellas versus las minucias almacenadas en el chip del documento electrónico.

Las minucias deben ser extraídas conforme al estándar **ISO/IEC 19794-2** Compact Card, sin cabezales, es decir, solamente la información de las minucias.

En este formato, cada punto característico de la huella dactilar se corresponde a una minucia, que a su vez es codificada en 3 bytes: uno para la coordenada X, otro para la coordenada Y, y un tercero para el tipo de punto (valle,

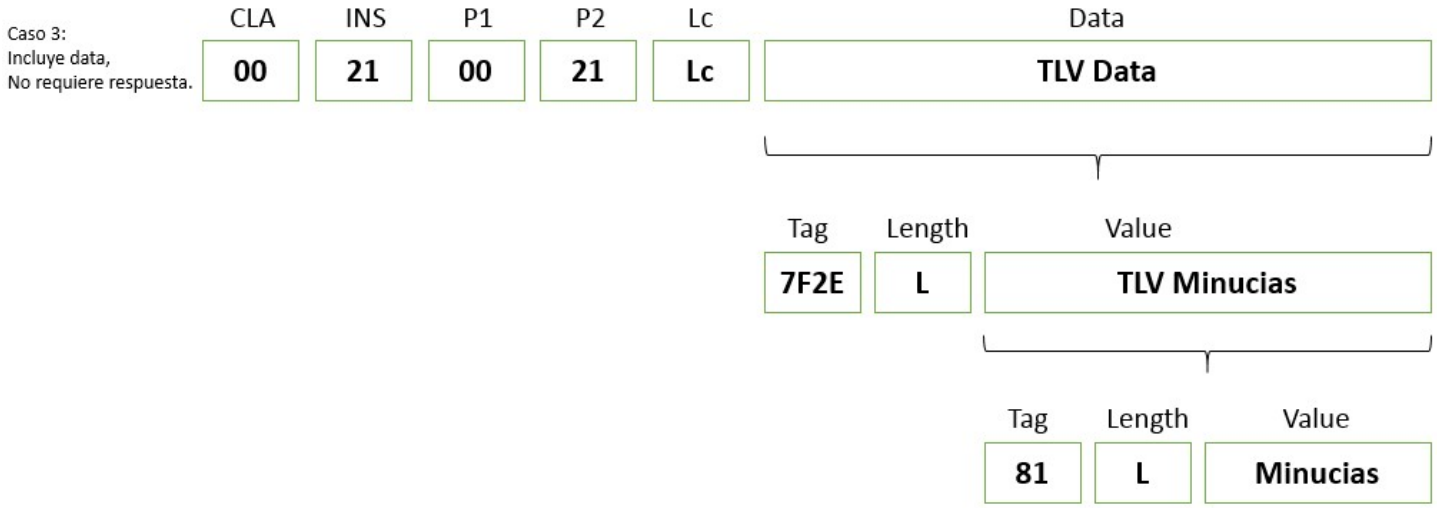
bifurcación, etc) y el ángulo de inclinación de la característica del mismo. En ese formato, un conjunto de minucias debe ser entonces siempre de una cantidad de bytes múltiplo de 3, de la forma:

X1|Y1|T1|X2|Y2|T2|....|Xn|Yn|Tn*(el | marca la división de bytes)*

Las minucias deben ordenarse ***primero ascendente por la coordenada Y*** y luego, en caso de dos minucias con igual Y, ***ascendente por la coordenada X***, de lo contrario el match fallará con error 6CXX (siendo XX la cantidad de intentos restante) o 6A80, que indica error de formateo de datos. Se recomienda tener especial cuidado con lenguajes de programación que manejen bytes con signo como java para la extracción de minucias. En esos casos, cualquier comparación susceptible al signo (< o >) debe ser hecha enmascarando los bytes con un *bitwise AND* (AND bit a bit, & en Java y C/C++) con 0xFF, lo cual fuerza a que sean considerados como bytes sin signo.

El largo máximo de las minucias soportado es de 192 bytes, es decir, 64 minucias de 3 bytes cada una.

Estructura del comando APDU para la operación *Match On Card*.



- **CLA:**
  - 00h Transmisión en plano
  - 0Ch Transmisión sobre canal seguro
- **INS:**
  - 21h Fijo para la operación de *Match on Card*.
- **P1:**
  - 00h Fijo para la operación de *Match on Card*.
- **P2:**
  - 21h Fijo para la operación de *Match on Card*.
- **Lc:**
  - Largo en bytes del TLV para validación *Match on Card.*
- **Data:**
  - TLV para la validación *Match on Card* que contiene las minucias extraídas de una huella.

Ejemplo de un comando APDU para verificación *Match On Card*:

IMPORTANTE: La cedula se bloquea luego de 5 intentos consecutivos de match on card sin éxito, devolviendo el error 0x6984

Las minucias para la versión 3 de los especímenes se solicitan a identificacion.electronica@agesic.gub.uy.

Extracción de los datos de identificación de la persona

Los datos de identificación de la persona dentro del eID son los que muestra el plástico (menos la imagen de la huella e imagen de la firma). Ver Cédula Electrónica (https://centroderecursos.agesic.gub.uy/web/seguridad/wiki?p_p_id=com_liferay_wiki_web_portlet_WikiPortlet&p_p_lifecycle=0&p_p_state=pop_up&p_p_mode=view&_com_liferay_wiki_web_portlet_WikiPortlet_mvcRenderCommandName=%2Fwiki%2Fedit_page&_com_liferay_wiki_web_portlet_WikiPortlet_redirect=https%3A%2F%2Fcentroderecursos.agesic.gub.uy%2Fweb%2Fseguridad%2Fwiki%2F-%2Fwiki%2FMain%2FGu%25C3%25ADa%2p_r_p_http%3A%2F%2Fwww.liferay.com%2Fpublic-render-parameters%2Fwiki_nodeId=33123&p_r_p_http%3A%2F%2Fwww.liferay.com%2Fpublic-render-parameters%2Fwiki_title=ci%2F%2Fapdu).

Estos datos se encuentran en archivos que deberán ser leídos con las operaciones *selectFile* y *readBinary*.

La información obtenida de las respuestas APDU a los comandos *readBinary* para cada archivo está codificada en formato TLV.

A continuación se presentan las operaciones de *selectFile* necesarias para la obtención de la información de identificación y la especificación de los TLV correspondientes a cada archivo.

Los datos del campo value se encuentran codificados en formato ASCII con excepción de la fecha de expedición.

selectFile del archivo que contiene el Número de documento, ID 7001:

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	00	02	70 01	Le

Información en formato TLV obtenida luego de las operaciones de *readBinary*:

Tag	Length	Value
5F01	09	NumeroDeDocumento

selectFile del archivo que contiene los datos biográficos, ID 7002:

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	00	02	70 02	Le

Información en formato TLV obtenida luego de las operaciones de *readBinary*:

Tag	Length	Value
1F01	L	PrimerApellido

Tag	Length	Value
1F02	L	SegundoApellido

Tag	Length	Value
1F03	L	Nombres

Tag	Length	Value
1F04	03	Nacionalidad (ISO 3166)

Tag	Length	Value
1F05	08	FechaDeNacimiento (DDMMAAA)

Tag	Length	Value
1F06	L	LugarDeNacimiento (Ciudad/Pais en ISO 3166)

Tag	Length	Value
1F07	08	NumeroDeCI

Tag	Length	Value
1F08	08	FechaDeExpedición (DDMMYYYY)

Tag	Length	Value
1F09	08	FechaDeExpiración (DDMMYYYY)

Tag	Length	Value
1F0A	L	Observaciones

selectFile del archivo que contiene la imagen en formato JPG, ID 7004:

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	00	02	70 04	Le

Información en formato TLV obtenida luego de las operaciones de *readBinary*: (Length = 2 bytes)

Tag	Length	Value
3F0182	L	ImagenJPG

selectFile del archivo que contiene el MRZ, ID 700B:

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	00	02	70 0B	Le

Información en formato TLV obtenida luego de las operaciones de *readBinary*:

Tag	Length	Value
7F01	L	MRZ

Firma Digital

Nota: Antes de ejecutar alguna operación de firma digital se debe haber ejecutado la operación de verificación de PIN

La operación de firma digital consta del cifrado de un hash utilizando la clave privada del documento electrónico y un algoritmo seleccionado. Los algoritmos soportados para la operación de firma digital son RSA y ECDSA, aunque actualmente las claves de la cédula electrónica son RSA de 2048 bits.

De forma macro los pasos para realizar la operación de firma son los siguientes:

1- Se realiza un hash del mensaje a firmar, el hash puede ser realizado de tres formas:

- Externo al eID (el más utilizado)
- Utilizando el eID
- Parcialmente externo y utilizando el eID.

2- Se selecciona el algoritmo de firma y hash utilizando el comando APDU *MSE_SET_DST*.

3- Se envía el hash al documento eID mediante el comando APDU *PSO_HASH*.

4- El hash es cifrado con la clave privada del documento eID utilizando el algoritmo y parámetros seleccionados en los pasos anteriores mediante el comando APDU *PSO–Compute Digital Signature*.

5-Se obtiene el hash cifrado como resultado del paso anterior.

Comando APDU *MSE_SET_DST*:

Caso 3:
Incluye data,
No requiere respuesta.

CLA	INS	P1	P2	Lc	Data
00	22	41	B6	Lc	TLV MSE_SET

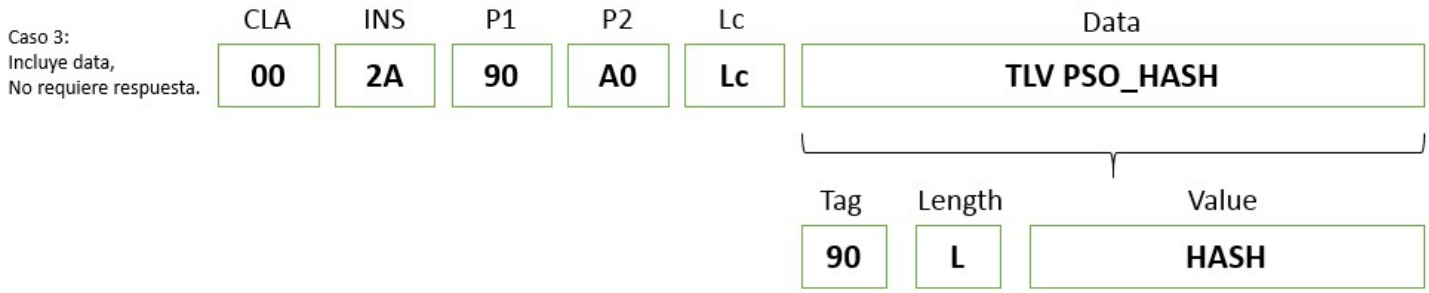
TLV			TLV		
TLV Key Reference			TLV Algo ID		
Tag	Length	Value	Tag	Length	Value
84	01	REF	80	01	ID

AlgoIDs:

01, 02, 03 = No hash
32, 35 = SHA224
41, 42, 45 = SHA256
52, 55 = SHA384
62, 65 = SHA512
x1=RSA padding ISO9796-2
x2=RSA padding PKCS#1v1.5
x3=RSA padding RFC2409
x5=RSA PSS

Por ejemplo para utilizar RSA con hash SHA-256 y padding PKCS#1v1.5 utilizaremos el AlgoID=42

Comando APDU *PSO_HASH*: (Hash realizado fuera de la tarjeta)



Comando APDU *PSO–Compute Digital Signature*:

Como la clave utilizada es RSA de 2048 bits se espera un resultado de largo 256 bytes = 0x100

Ejemplo de firma digital

A continuación se presenta como ejemplo los comandos APDU enviados para la firma digital de un hash de un mensaje generado de forma externa con el algoritmo SHA-256.

Mensaje a firmar: "Ejemplo de firma en APDU utilizando el nuevo documento eID"
HASH en formato hexadecimal del mensaje con el algoritmo SHA256:
"A3D00CBE708B435D6E7B898770378FD54319B2FD7571C769DB414094E7008624".

MSE_SET_DST:

PSO_HASH:

CLA	INS	P1	P2	Lc	Data
00	2A	90	A0	20	A3D00CBE708B435D6E7B898770...

PSO-Compute Digital Signature:

CLA	INS	P1	P2	Le
00	A4	9E	9A	100

Hash cifrado con la clave privada del documento eID obtenido como resultado al comando PSO-CDS: "A91283AA1239213...".

Repositorios públicos de ejemplo

Existen estos dos desarrollos públicos en Github que utilizan APDUs.

Diferentes servicios con APDU https://goo.gl/KvFht2 (https://goo.gl/KvFht2)

Un ejemplo de uso con interfaz gráfica, lee los datos públicos de la CI y los muestra en pantalla https://goo.gl/FAfe4X (https://goo.gl/FAfe4X)

5793 Accesos

Promedio (1 Voto)

★★★★★

archivos adjuntos

PNG apdu_readBinary.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_ent…

PNG apdu_IsverifyPin.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_ent…

PNG apdu_selectIAS.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entr…

PNG apdu_PSO_HASH.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_casos (2).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entry/…

PNG apdu_comando_MOC (1).png (https://centroderecursos.agesic.gub.uy/documents/portlet_…

PNG apdu_casos.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entry/3…

PNG apdu_selectFile.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entr…

PNG apdu_UserID_7000.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_…

PNG apdu_comando (2) (1).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file…

PNG apdu_comando (1).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_respuesta.png (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entry…

PNG apdu_PSO_CDS_comando (1).png (https://centroderecursos.agesic.gub.uy/documents/p…

PNG apdu_PSO_HASH (1).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file…

PNG apdu_MSE_SET_DST.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_fil…

PNG apdu_selectFile2_2.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_…

PNG apdu_UserID_7004.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_…

PNG apdu_comando (3).PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_MSE_SET_DST_comando.PNG (https://centroderecursos.agesic.gub.uy/document…

PNG apdu_UserID_7001.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_…

PNG apdu_PSO_HASH (3).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file…

PNG apdu_UserID_700B.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_…

PNG apdu_PSO_CDS.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_ent…

PNG apdu_comando (2).PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_readBinary_1.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_…

PNG apdu_selectIAS_1.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_TLV_DatosBiograficos_1.PNG (https://centroderecursos.agesic.gub.uy/documents/…

PNG apdu_comando_MOC_1.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet…

PNG apdu_PSO_CDS_comando.PNG (https://centroderecursos.agesic.gub.uy/documents/port…

PNG apdu_TLV_MRZ.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_ent…

PNG apdu_comando (1).PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_PSO_HASH_ejemplo.PNG (https://centroderecursos.agesic.gub.uy/documents/port…

PNG apdu_TLV_docnumber.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_fil…

PNG apdu_casos (1).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entry/…

PNG apdu_PSO_HASH (2).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file…

PNG apdu_verifyPin.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entry…

PNG apdu_respuesta (2).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_TLV_DatosBiograficos.PNG (https://centroderecursos.agesic.gub.uy/documents/por…

PNG apdu_UserID_7002.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_…

PNG apdu_respuesta (1).png (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_comando_MOC (2).png (https://centroderecursos.agesic.gub.uy/documents/portlet_…

PNG apdu_IsverifyPin_1.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_…

PNG apdu_PSO_CDS_comando2.PNG (https://centroderecursos.agesic.gub.uy/documents/po…

PNG estructuraUserIdentification.png (https://centroderecursos.agesic.gub.uy/documents/portl…

PNG apdu_comando.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entr…

PNG FCI.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_entry/31564/FCI…

PNG apdu_TLV_imagenJPG.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_f…

PNG apdu_selectFile2.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_ent…

PNG apdu_comando_MOC.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_fil…

PNG apdu_selectFile_1.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_e…

PNG apdu_verifyPin_1.PNG (https://centroderecursos.agesic.gub.uy/documents/portlet_file_en…