

Proyecto: **ADQUISICIÓN DE TARJETAS INTELIGENTES SMART CARD PARA EL DNIE**

Llaves y Certificados - Comandos APDU

Doc. No:	2025_0014
Versión:	1.0
Fecha:	02 de julio de 2025



**CONSORCIO IN CONTINU ET SERVICES S.A.S. SUCURSAL DEL PERÚ -INVERSIONES SAN
MANUEL S.A.C.-SELP S.A.S.**

Contenido

Contenido

1	Firma digital.....	3
1.1	Selección del applet IAS(Identification, Authentication and Signature).....	3
1.2	Selección del Application Dedicated File de PKI.	3
1.3	Consultar intentos PIN.....	4
1.4	Verificación del PIN de firma.....	5
1.5	Preparación del Security Environment para Firma.	5
1.6	Firma.....	6
2	Cifrado con llave de autenticación.....	6
2.1	Selección del applet IAS.....	6
2.2	Selección del ADF de PKI.	7
2.3	Verificación del PIN de autenticación.	7
2.4	Preparación del Security Environment para autenticación.....	8
2.5	Cifrar con llave de autenticación.	8
3	Descifrado con llave de cifrado.....	9
3.1	Selección del applet IAS.....	9
3.2	Selección del Application Dedicated File de PKI.	9
3.3	Verificación del PIN de cifrado.	10
3.4	Preparación del Security Environment para descifrado.	10
3.5	Descifrado.	11
4	Obtención de certificados.....	11
4.1	Selección del applet IAS.....	11
4.2	Selección del ADF de PKI.	12
4.3	Selección de un certificado.	12
4.4	Obtención del certificado.....	13
5	Match on Card.	15
5.1	Selección del applet IAS.....	15
5.2	Match on Card	16

Introducción

Este documento brinda el detalle de los comandos APDU, para la realización de operaciones criptográficas, con el nuevo DNI electrónico versión 3.

El DNI cuenta con tres certificados con su correspondiente par de llaves (pública y privada), los cuales son:

- Certificado y par de llaves para firma digital.
- Certificado y par de llaves para autenticación.
- Certificado y par de llaves para cifrado.

A diferencia de los certificados que se pueden leer sin restricción, las llaves privadas están protegidas por un PIN. Para hacer uso de dichas llaves se tiene que realizar una verificación de credenciales, tal como se muestra en la siguiente tabla:

Llave privada	Tipo de protección
Firma	PIN Auth
Autenticación	PIN Auth
Cifrado	PIN Auth

1 Firma digital.

Para realizar una firma digital, se debe hacer uso de la llave privada de firma digital. Se debe ejecutar en el siguiente orden:

1.1 Selección del applet IAS(Identification, Authentication and Signature)

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
A000000077030C60000000FE00000500		AID del applet IAS

Por ejemplo:

APDU>>>:00A4040C10A000000077030C60000000FE00000500

APDU<<<<:9000

1.2 Selección del Application Dedicated File de PKI.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
E828BD080FD25047656E65726963		AID del ADF PKI

Por ejemplo:

APDU>>>>:00A4040C0EE828BD080FD25047656E65726963

APDU<<<<:9000

1.3 Consultar intentos PIN.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	20h	VERIFY PIN
P1	00h	Constante
P2	03h	Indica el número de referencia del PIN.

Por ejemplo:

APDU>>>>: 00200003

APDU<<<<:63C5

Donde 5 es Intentos restantes de PIN

1.4 Verificación del PIN de firma.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	20h	Verify PIN
P1	00h	Constante
P2	03h	Indica el número de referencia del PIN.
Lc	0C	Indica la longitud del PIN
DATA		DETALLE
31323334FFFFFFFFFFFFFFFF		PIN ASCII en hexadecimal, 12 bytes.

Por ejemplo:

APDU>>>>:

002000030C31323334FFFFFFFFFFFFFFFF

APDU<<<<:9000

1.5 Preparación del Security Environment para Firma.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	22h	MANAGE SECURITY ENVIRONMENT
P1	41h	Constante
P2	B6h	Constante
DATA		DETALLE
84h 82h 80h 42h		Donde: 0x82: Asymmetric key (private portion) reference, llave privada de firma. 0x42: Algorithm identifier for Data Signature, RSA PKCS#1 v1.5 - SHA-256.

Por ejemplo:

APDU>>>>:002241B606840182800142

APDU<<<<:9000

1.6 Firma.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	2Ah	PERFORM SECURITY OPERATION
P1	9Eh	Sign
P2	9Ah	Constante
Lc field	20h	0x20 for SHA-256
DATA		DETALLE
<DATA>		Data o hash a firmar en hexadecimal, en SHA-256

Por ejemplo:

APDU>>>>:002A9E9A20F8CA015AC7305A753534FF52C2AD2EC198FCDB7522BE92747732AFF0C771847C

APDU<<<<:A2B4DA4C5C8138D61BA22A071F91F25948B0D43728F21904DC988CEDEFFD878D925FD913F4BFB7C0F1F38CDA54AFD35EED6550832EAD42948967DA9D8B0B143FAA1DB0A971C19119463C674B70964D4B3EF16757B9EA99C3CBE81AB47FEE32EF7D126EFC751343778C69575BCADAAED97C9C4A7520DE40DA409FDE785E840277D332232CB9060F8C3365D30B19DAAFBBBD855A81D7F576CA445D67FE10F85E30B6F75C3AAB9ADEC8AA27AA45B092BF809CDBC622C95A1C390B493C10102612CCE0DEF12CE8E732EBDA47D0E406F4A28D1FCF9F884982D83F78A0189EDD40F876CBC05EEB9220A95DF4D630FDC38F111526C40CDFC56E9D1DE7157A4150490C6F9000

2 Cifrado con llave de autenticación.

Para realizar un cifrado con la llave de autenticación, se debe ejecutar en el siguiente orden:

2.1 Selección del applet IAS.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
A000000077030C60000000FE00000500		AID del applet IAS

Por ejemplo:

APDU>>>>:00A4040C10A000000077030C60000000FE00000500

APDU<<<<:9000

2.2 Selección del ADF de PKI.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
E828BD080FD25047656E65726963		AID del ADF PKI

Por ejemplo:

APDU>>>>:00A4040C0EE828BD080FD25047656E65726963

APDU<<<<:9000

2.3 Verificación del PIN de autenticación.

Para poder acceder a la llave privada de autenticación se puede realizar una verificación con el PIN.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	20h	Verify PIN
P1	00h	Constante
P2	03h	Indica el número de referencia del PIN.
DATA		DETALLE
31323334FFFFFFFFFFFFFFFF		PIN ASCII en hexadecimal, 12 bytes.

Por ejemplo:

APDU>>>>:

002000030C31323334FFFFFFFFFFFFFFFF

APDU<<<<:9000

2.4 Preparación del Security Environment para autenticación.

CAMPO		VALOR	DESCRIPCIÓN
CLA		00h	Comando estándar
INS		22h	MANAGE SECURITY ENVIRONMENT
P1		41h	Constante
P2		A4h	Constante
DATA			DETALLE
	84h	81h	Donde 0x81 es RSA para la llave de autenticación sin padding.
	80h	02h	
			0x02 para RSA PKCS#1 v.15

Por ejemplo:

APDU>>>>: 002241A406840181800102

APDU<<<<:9000

2.5 Cifrar con llave de autenticación.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	88h	MANAGE SECURITY ENVIRONMENT
P1	00h	Constante
P2	00h	Constante
Lc field	variable	variable
DATA		DETALLE
<DATA>		Data a cifrar en hexagesimal

Por ejemplo:

```
APDU>>>>: 0088000008313233343536373800
APDU<<<<:319B5A0DFE5C74B01965A1780AD8DC799F4A47C4B8C17943990021FA6DD972FEBAB26854A72A58070B
DC6492FB83EEEEF95F7B37907AD7BA456566B034DE4604C9189DF74EEFEED85CA33BB99ED46C5F9A5C7FB662E0
AB631BD7AF3AC3F9BE0AC7E66F2A63E805C4C3C0FE7E583328707129897DEF4F34289F9DF53D6B4EA6A5E03E9A
DAC7024ADC240FC6D608C8B898A6FE65190401132293FE4F1538E3A3E667CA96A4BEA2A0E964FA875A9458FFF94
34D98E6C9CA0F40FE8A61FD3DD4D6990366B2303350CEED5A099E438B3A93CB44580E4873A9E8FF7B784DBDC99
987D9D79B698AB84585AACDD8A3607E7BA357157AB9413D185C2C3477B774A78F367389000
```

3 Descifrado con llave de cifrado.

Para realizar un descifrado con la llave de cifrado, se debe ejecutar en el siguiente orden:

3.1 Selección del applet IAS.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
A000000077030C60000000FE00000500		AID del applet IAS

Por ejemplo:

```
APDU>>>>:00A4040C10A000000077030C60000000FE00000500
```

```
APDU<<<<:9000
```

3.2 Selección del Application Dedicated File de PKI.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
E828BD080FD25047656E65726963		AID del ADF PKI

Por ejemplo:

```
APDU>>>>:00A4040C0EE828BD080FD25047656E65726963
```

```
APDU<<<<:9000
```

3.3 Verificación del PIN de cifrado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	20h	Verify PIN
P1	00h	Constante
P2	03h	Indica el número de referencia del PIN.
DATA		DETALLE
31323334FFFFFFFFFFFFFFFF		PIN ASCII en hexadecimal, 12 bytes.

Por ejemplo:

APDU>>>>:

002000030C31323334FFFFFFFFFFFFFFFF

APDU<<<<:9000

3.4 Preparación del Security Environment para descifrado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	22h	MANAGE SECURITY ENVIRONMENT
P1	41h	Constante
P2	B8h	Constante
DATA		DETALLE
84h 83h 80h FF300100h		Donde 0x83 hace referencia a la llave privada de cifrado. FF300100 hace referencia a RSA PKCS#1 v1.5

Por ejemplo:

APDU>>>>: 002241B8098401838004FF300100

APDU<<<<:9000

3.5 Descifrado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	2Ah	PERFORM SECURITY OPERATION
P1	80h	Descifrado
P2	86h	Constante
Lc Field	Variable	Longitud de la data
DATA		DETALLE
81h<DATA>		Donde <DATA> es la data a descifrar

Por ejemplo:

```
APDU>>>>:002A8086000101819FBD1E4C59DE56416311AC87B41487615492E3799B3998CDE17BED21D6647109F8A
19F1519CFE03FF663ADF36AA3750743A9D4B776977F9B8716F238AE8D62B88CB7CB34AE9485701EDA90872580638
A5DF27669329ACA21EEDAFEB3A09CD9522F67AF1A2A1B66BA869357D6AB17FA7C9C7B23EACCEEC991D0FF438E
3F402A47DDF184E351A1615EA0479AB07B521AD4F7ADA87AE9664A0269E96B7F19A9D32D96BE43AB595EDD3C66
1189F3BBE8C5065AC8543C436CAA31B9FCD3795ADE3335C6804F2FDEBD5000C4410CFABCFFACB4812BA104370
BD84AB94F53CD3CCA012DE4F5EE8DC2E6899845786AC42C75A54195C4C1B8D81A2AB279832DD166796D660100
```

```
APDU<<<<: 31323334353637389000
```

4 Obtención de certificados.

Para obtener los certificados, se debe ejecutar en el siguiente orden:

4.1 Selección del applet IAS.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
A000000077030C60000000FE00000500		AID del applet IAS

Por ejemplo:

```
APDU>>>>:00A4040C10A000000077030C60000000FE00000500
```

```
APDU<<<<:9000
```

4.2 Selección del ADF de PKI.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
E828BD080FD25047656E65726963		AID del ADF PKI

Por ejemplo:

APDU>>>>:00A4040C0EE828BD080FD25047656E65726963

APDU<<<<:9000

4.3 Selección de un certificado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	02h	Constante
P2	04h	Constante
Lc field	02h	Longitud del ID del certificado.
DATA		DETALLE
<ID FILE>		Donde <ID FILE> es el identificador del certificado> CE81: Certificado de Autenticacion CE82: Certificado de firma CE83: Certificado de cifrado

Por ejemplo:

APDU>>>>: 00A4020402001D

APDU<<<<:9000

4.4 Obtención del certificado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	B1h	READ BINARY
P1	(offset >> 8) & 0xFF	Byte alto del desplazamiento (offset).
P2	offset & 0xFF	Byte bajo del desplazamiento (offset).
DATA		DETALLE
<offset>		Donde <offset> es los bytes (codificado en dos bytes) desde el cual se leerá los bytes restantes inclusive.
NE	FFh	Máximo número de bytes esperados en la respuesta.

Respuesta	DETALLE
<binary>	Donde < binary> es los bytes del certificado. Esta longitud se debe tomar como referencia para calcular el nuevo offset.

Se debe ejecutar de forma iterativa hasta que la tarjeta responda con el "Status Word" fin de archivo (6282).

Por ejemplo:

APDU>>>>: 00B00000FF

APDU<<<<:308208D4308206BCA0030201020214620A5462F1C48C057609C52CB49AF6EC03291520300D06092A864886F70D01010B05003072310B3009060355040613025045313C303A060355040A0C33526567697374726F204E6163696F6E616C206465204964656E7469666963616369C3B36E20792045737461646F20436976696C3125302306035504030C1C454345502D52454E49454320436C617373203220545249414C204949301E170D3235303631383137353930335A170D3235303732383137353930335A3081EC310B30090603550406130250453112301006035504080C094C696D612D4C9000

APDU>>>>: 00B000E7FF

APDU<<<<:696D61310F300D06035504070C06427265C3B161311E301C060355040B0C15455245505F504E5F52454E4945435F383734353531311A301806035504040C1153414E54494C4C414E41204855414D414E31153013060355042A0C0C524F42494E47205045524359311730150603550405130E504E4F50452D3130373134353130314C304A06035504030C437C7C534F4C4F20505255454241537C7C2053414E54494C4C414E41204855414D414E20524F42494E4720504552435920505F434946203130373134353130206861726430820122300D06092A864886F70D01010105000382010F00309000

APDU>>>>: 00B001CEFF

APDU<<<<:82010A0282010100A838816483A868155638D1D9E61CBF130C981AF07443F979129FF3D69FB25BDD45E4EC9BBED1B664250D3E46E3FC96CC1209E1CA2CB2A761E90949CA739B2FFB4BDF373C873A46DC37267F94D8D0C81636BF577C1F31BACCD207EED3F17F7E6AA0084DB829DA2A77CE44EE901D67F25E919EEECB26029545E023222F39621A8924820FFF7B578D57595801AAAE9306B5B8CA6ED8D6833D8E0C1A2CBD9BFD1AB1A04BBCDE00F2435A2FDAF7C5BD9B011366B355AB6DE2903D0A17A6B26A483BC0F0643E904FAA524B9B4E5A31B3A24C6054146B7E5738D7F984338EDDD310C9000

APDU>>>>: 00B002B5FF

APDU<<<<:EE12B1BD4A325CA69CF049EB38067BA50F98A9AA87C74491C4D93E47486E3CC85B0203010001A38203E5308203E1300C0603551D130101FF04023000301F0603551D23041830168014F29A001F8B95B0D9E0512F64A934A8D813823467305306082B0601050507010104473045304306082B060105050730028637687474703A2F2F63726C2E72656E6965632E676F622E70652F74726C742F736861322F6361636C617373325F747269616C69692E637274308202CB0603551D20048202C2308202BE30819B06112B06010401829364020103010065876800308185303106082B0601050507029000

APDU>>>>: 00B0039CFF

APDU<<<<:01162568747470733A2F2F7777772E72656E6965632E676F622E70652F7265706F7369746F72792F305006082B0601050507020230441E420050006F006C00ED0074006900630061002000470065006E006500720061006C00200064006500200043006500720074006900660069006300610063006900F3006E3081C306112B060104018293640201030100678768003081AD303106082B06010505070201162568747470733A2F2F7777772E72656E6965632E676F622E70652F7265706F7369746F72792F307806082B06010505070202306C1E6A004400650063006C0061007200610063009000

APDU>>>>: 00B00483FF

APDU<<<<:6900F3006E00200064006500200050007200E100630074006900630061007300200064006500200043006500720074006900660069006300610063006900F3006E00200045004300450050002D00520045004E0049004500433081AE060604008F7A01023081A33081A006082B060105050702023081931E81900050006F006C00ED007400690063006100200064006500200043006500720074006900660069006300610064006F0020004E006F0072006D0061006C0069007A00610064006F0020004E00430050002B0020006400650020006100630075006500720064006F00200063006F009000

APDU>>>>: 00B0056AFF

APDU<<<<:6E0020004500540053004900200045004E0020003300310039003400310031002D00313081A606112B06010401829364020103040267876C0230819030818D06082B060105050702023081801E7E0043006500720074006900660069006300610064006F0020004400690067006900740061006C002000700061007200610020007000720075006500620061007300200043006C006100730073002000320020006400650020004300690066007200610064006F00200065006E00200068006100720064007700610072006530130603551D25040C300A06082B0601050507030430480603551D9000

APDU>>>>: 00B00651FF

APDU<<<<:1F0441303F303DA03BA0398637687474703A2F2F63726C2E72656E6965632E676F622E70652F74726C742F736861322F6361636C617373325F747269616C69692E63726C301D0603551D0E04160414A70023051244B8CD759E23D857F6E65443071259300E0603551D0F0101FF040403020410300D06092A864886F70D01010B050003820201004D0EC14B26566D6DB4B3398594BEF71E443423804333AF830D0482E7F6BE460A55F28380FB8A8AB53F8FA8AF26DAEFA65A2CBDD7311ED4B71B76CE9EDF107A70E32C9173C267BD5F48D45A20E6908C28953CE9579DF37FA46F33A837815F37A19000

APDU>>>>: 00B00738FF

APDU<<<<:9663D9F6D9A34AFC72908F9665A9FEADF0FE6BB3772AD7CF595C09660ADFEB7108B92A4C3816210073493B575C6A40A664709E5FAD259AD0DE3155C5CD135DB45156BBBD794450BCFAE09A71EBCD7DCA766ED3EF8223D3633716BB2800EEAD35EFEDD99CDA806465AD847A2B1B71280B954E23F7575AED7EE21EE09826D5217903C245188D1BFACCF2122ACEF6E1C1726E72D74CE3C89915D52CFBB31207A6013220422C436AFCA278B16C1141A93D2658922FB2C3F8189C4B7B289ED08324E7CD5CE1FE411331268D80F2FAD65C56F526E3DEF3CF82FDB2828AF2BC240BBE9E499276C4D987F1959000

APDU>>>>: 00B0081FFF

APDU<<<<:065DA8CE8C231CAEB3198FA65C7E27D2FB2BD352947E7161722E7082A825E07D85C092CFA35C6C7E4A62DC25145A621B55C715205057E15306064046B70B56402821FCE60484A380F6D701426D8B2845FF7D49B8A162A4CABAC22DF5ACC33F981B5C463B980B3C7B69FB20E47EB1C3C7D81CFC84D7D7FEB148DFB467F4FC8AA161C53F8286F738FFF57D27962A4F87C30A2BB03A0D8A16F4422323921F87D1F3D318C0EC6F624A52DACADA906D4728BCCB2BDD3F17551486576282

5 Match on Card.

Para realizar Match on Card seguir los siguientes pasos

5.1 Selección del applet IAS.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	0Ch	Constante
DATA		DETALLE
A000000077030C60000000FE00000500		AID del applet ID-A

Por ejemplo:

APDU>>>>:00A4040C10A000000077030C60000000FE00000500

APDU<<<<:9000

5.2 Match on Card

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	21h	BIOMETRY
P1	00h	Constante
P2	06h	Constante
Lc Field	Variable	Longitud en hex de la <DATA>
DATA		DETALLE
7F2Eh	81h <ISO TEMPLATE>	Se envía un TLV, donde <ISO TEMPLATE> es la minucia en ISO Compact Card.

Por ejemplo:

APDU>>>>:

```
00210006E27F2E81DE8181DB7E0E9E8B249D6A2681592DA5733563A1385B933A7B804060674584CA4F79655284895
57B3757A8D95B974F5DA86360A64B65498E669B81697B6E73A9BD75B5B37897807861A67AB521808C4B81AAC486B
38E8F6F55906D4795AC299EAB849E6A789F557B9F6896A06EA5A1AE2EA3AC5EA372D6A57351A7AF8DA86B49A96
D58AC71CEB2AFB3B36EDCB9B070BA6026BB8D5CBC958BC368CDCA4D3BCDAAD2CF4A43D38C5CD46352D44431
D689C4D98939DA4A47DF89A2DF89D6E04763E0428EE349B3E389C5E5874FE64573E8A261EE6363F384BBF5844CF
8458BFE84
```

APDU<<<<:9000