Llaves y Certificados - Comandos APDU

Nueva Tarjeta de DNI – Electrónico

Diciembre - 2019

Contenido

Introducción

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

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 o BIO (huella dactilar). 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 de firma
Autenticación	PIN de autenticación o BIO
Cifrado	PIN de cifrado

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 de la aplicación de PKI.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	00h	Constante
DATA		**DETALLE**
E828BD080FD25047656E65726963		AID de la aplicación PKI

Por ejemplo:

APDU>>>>:00A404000EE828BD080FD25047656E65726963

APDU<<<<:9000

1.2 Verificación del PIN de firma.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	20h	VERIFY PIN
P1	00h	Constante

P2	81h	Codificación del SDO del PIN de firma.
DATA		**DETALLE**
3131313131313131		PIN ASCII en hexadecimal.

Por ejemplo:

APDU>>>>:00200081083131313131313131

APDU<<<<:9000

1.3 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**
80h 8Ah **84h** 81h		Donde 0x8A es RSA para firma con PKCS#1 padding y off-card hash.

Por ejemplo:

APDU>>>>:002241B60680018A840181

APDU<<<<:9000

1.4 Firma.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	2Ah	PERFORM SECURITY OPERATION
P1	9Eh	Sign
P2	9Ah	Constante
DATA		**DETALLE**
<DATA>		Data o hash a firmar en hexadecimal.

Por ejemplo:

APDU>>>>:002A9E9A2830303031303230333034303530363037303830393061306230633064306530663130313131323133

APDU<<<<:76208A9518FAD64C8D2F757532CFA098008A0507E9542D4F95A19BE49ACAEA24C60610
6A7E0F31A4E3779EC1C49CE9D1655F54139C63D219B9180B16B6C77730784D6CF6885B440E6B852
2B27AF5BEB428F3841450295536710AB1DDE8C48B61FA4846D0AB6A1F3E842C5A24CDC4D69734D
5843E36D0B4056D814A2EA29C1CD88720589024AF8F922C2CCEC7B25B585EFCD942F29A5EA3077
C8CF8EFEB7DEDBCDD4ADE98030B2A847E02C6C2744A113FB9F515384E4A5FFC0A6F4C04FCFDC
C02A648F968100BA3D6DEE2B683C53ACD12C5FEF6E75C9CE04CCC351CF25D0F25136E6454847C
CDF63E7B4A46F6A8987B5C9F4EA075DB8C4BB31D4DEF51BEDCC1929000

2 Descifrado con llave de autenticación.

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

2.1 Selección de la aplicación de PKI.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	00h	Constante
DATA		**DETALLE**
E828BD080FD25047656E65726963		AID de la aplicación PKI

Por ejemplo:

APDU>>>>:00A404000EE828BD080FD25047656E65726963

APDU<<<<:9000

2.2 Verificación del PIN de autenticación o BIO.

Para poder acceder a la llave privada de autenticación se puede realizar una verificación con el PIN o una verificación con el BIO de 1 a N (Significa que se puede hacer uso de cualquier dedo de la mano derecha o izquierda para realizar el “match on card”):

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	20h	VERIFY PIN
P1	00h	Constante
P2	82h	SDO del PIN de autenticación.
DATA		**DETALLE**
3232323232323232		PIN ASCII en hexadecimal.

Por ejemplo:

APDU>>>>:00200081083232323232323232

APDU<<<<:9000

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	21h	BIOMETRY
P1	02h	Constante
P2	81h	SDO del BIO.
DATA		**DETALLE**
7F2Eh **81h** <ISO TEMPLATE>		Se envía un TLV, donde <ISO TEMPLATE> es la minucia en ISO Compact Card.

Por ejemplo:

```
APDU>>>>:00210281F17F2E81ED8181EA8202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5
CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB175820
2BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5
CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB175820
2BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5
CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0E5CCB175820
2BC9B0E5CCB1758202BC9B0E5CCB1758202BC9B0
```

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

2.3 Preparación del Security Environment para descifrado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	22h	MANAGE SECURITY ENVIRONMENT
P1	41h	Constante
P2	B6h	Constante
DATA		**DETALLE**
80h 8Ch **84h** 82h		Donde 0x8C es RSA para descifrado sin padding.

Por ejemplo:

```
APDU>>>>:002241B80680018C840182
```

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

2.4 Descifrado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	2Ah	PERFORM SECURITY OPERATION

P1	80h	Descifrado
P2	86h	Constante
DATA		**DETALLE**
81h<DATA>		Donde <DATA> es la data a descifrar

Por ejemplo:

APDU>>>>:002A8086000101816612E7B0369C6485A4CBD6CF92020302AFBEC4AC3351C26BFD3585
0379736AAD1ED3C60CE21B2D6A631C644971FE4AE7AE394DB3F1068A87368BE3D746F7E810A606
7038265E3AA057BF1DB2DAEF64AF15D663453DBBE93B9A217837BBA073B4303FA1C0FEAD71A703
6DEAD8DDCA6670BA570349948495CF82792FF7A7E51BE32FEFF40864C984CB655C85993F36590FE
F0FE59206E3E4BCDE74CE7E1B868C082A948384F8C96932D7BACED2BBEB559683840718D2924F4
46D6099ADCA95D770D3EA6BC5E00B7AFD4C9E0896D65A9799A2965349D2B3353D4724F800060DA
0E1A07B9F314421D4083B8C0651FBEA19C38D0C16C49B771BCF9C7FCC811CFFE3B9

APDU<<<<:00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000048454C4C4F20574F524C
44204D4553534147459000

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 de la aplicación de PKI.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	00h	Constante
DATA		**DETALLE**
E828BD080FD25047656E65726963		AID de la aplicación PKI

Por ejemplo:

APDU>>>>:00A404000EE828BD080FD25047656E65726963

APDU<<<<:9000

3.2 Verificación del PIN de cifrado.

CAMPO	VALOR	DESCRIPCIÓN

CLA	00h	Comando estándar
INS	20h	VERIFY PIN
P1	00h	Constante
P2	83h	SDO del PIN de cifrado.
DATA		**DETALLE**
3333333333333333		PIN ASCII en hexadecimal.

Por ejemplo:

APDU>>>>:00200083083333333333333333

APDU<<<<:9000

3.3 Preparación del Security Environment para descifrado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	22h	MANAGE SECURITY ENVIRONMENT
P1	41h	Constante
P2	B6h	Constante
DATA		**DETALLE**
80h 8Ch **84h** 83h		Donde 0x8C es RSA para descifrado sin padding.

Por ejemplo:

APDU>>>>:002241B80680018C840183

APDU<<<<:9000

3.4 Descifrado.

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

Por ejemplo:

APDU>>>>:002A8086000101816AA7BEFD1E00FF488A1B49019F9E778AE8C42FAE84FB9B2E57931A
298B2654C8E8421E9229DA50C4663A2DB5570CEB061799E0288A576ECA54CBDBC9AA4BB978FC1F

5DE69F66D019C9F97DF469A7FB590941632DF77EEF392AC093535CA20ABE6FBDE752B289639ECA
63B5C580D2D80D507E85897B642DB620548E7935B2BC87744F614FE8B41D984486F39AE28A01671
E75393EC9A443F66E9BD74BB854B03B0F867F87A52AD336F76BAE7AD4C0DAE49B00CD0BD522C8
4267A885CB389AB27E9EECAADFEA7CD505E42E014CAB97EADB2AC39466B44B75F7288D6E4E28F
C37ACEDC1818B75ED8A20430009761C12973D8B0A492C0D0743A4EB5346A7C37CEAA9

APDU<<<<:000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000048454C4C4F20574F524C
44204D4553534147459000

4 Obtención de certificados.

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

4.1 Selección de la aplicación de PKI.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	04h	Constante
P2	00h	Constante
DATA		**DETALLE**
E828BD080FD25047656E65726963		AID de la aplicación PKI

Por ejemplo:

APDU>>>>:00A404000EE828BD080FD25047656E65726963

APDU<<<<:9000

4.2 Selección de un certificado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	A4h	SELECT FILE
P1	02h	Constante
P2	04h	Constante
DATA		**DETALLE**

<ID FILE>	Donde <ID FILE> es el identificador del certificado: 001D: Certificado de Firma. 001C: Certificado de autenticación. 001B: Certificado de cifrado.

Por ejemplo:

APDU>>>>: 00A4020402001D

APDU<<<<:9000

4.3 Obtención del certificado.

CAMPO	VALOR	DESCRIPCIÓN
CLA	00h	Comando estándar
INS	B1h	READ BINARY ENHANCED
P1	00h	Constante
P2	00h	Constante
DATA		**DETALLE**
54h <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
53h <binary>	Como resultado tenemos una respuesta TLV con el Tag 53, donde < binary> es los bytes del certificado. Esta longitud se debe tomar como referencia para calcular el nuevo offset y que debe ser una longitud de 00E4 (codificación en dos bytes).

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

Por ejemplo:

APDU>>>>:00B100000454020000FF

APDU<<<<:5381E43082098130820769A0030201020208573A3D3AF6C9672E300D06092A864886F70D
01010B0500306C310B3009060355040613025045313C303A060355040A0C33526567697374726F204E
6163696F6E616C206465204964656E7469666963616369C3B36E20792045737461646F20436976696C3
11F301D06035504030C16454345502D52454E49454320434120436C6173732032301E170D313930393
0343136323833335A170D313931303134313632383333335A3081E4310B3009060355040613025045311
3010060355040800C094C494D412D4C494D41310D300B06035504070C044C9000

APDU>>>>:00B1000004540200E4FF

APDU<<<<:5381E4494D41311C301A060355040B0C13455245505F504E5F454345505F5030303030323
1183016060355040C0F504F52545547414C20564152474153311530130603550420C0C5061756C6
F2043C3A97361723117301506035040513E504E4F50452D343436323737383030314A30480603550403
0C417C7C534F4C4F20505255454241537C7C20504F52545547414C20564152474153205061756C6F20
43C3A973617220505F4649522034343632373738302068617264308201223000D06092A864886F70D010
10105000382010F003082010A0282010100BC32B6E2C08987D863F7BFBE9000

APDU>>>>:00B1000004540201C8FF

APDU<<<<:5381E4679C192E5B2B82312354AB8BF13686332759E2631AD5C1E3A0E90996F7FA281C9
912AB2865980EA505AF2206D9905B253C0AC7AEBD018651BBE0C47116716C405D36E1ED9B9D610
2116A9BC7BDB16DC6F2942E2EC947368EF668EB64886DD92D9187E47829E820C585753165B16A6E
6A9199145C8B1227E61376476B673E13AB296E00A170F68F17D578A656F6C393358B0DD020779CE8
12479C09D2BDFAB437F47BDAA9E58C9DE842B22D38EEA4F82BCE4633D5A5DD129A2D65861527C
07AC5F5E4B6CA62F0672A37C481641F96BA060DA9DDD4CA8F8E0287B5255A8D653770CB35C4149
000

APDU>>>>:00B1000004540202ACFF

APDU<<<<:5381E4F7D6AB8601CBA7D9B76F6CDA568B41B30203010001A38204AC308204A8307106
082B060105050701010465306330 3A06082B06010505073002862E687474703A2F2F7777772E72656E6
965632E676F622E70652F6372742F736861322F6361636C617373322E637274302506082B0601050507
30018619687474703A2F2F6F6373702E72656E6965632E676F622E7065301D0603551D0E0416041422
4C00E5A9A28D5E561F333CB50A1C3D8BF4FA53300C0603551D130101FF04023000301F0603551D23
04183016801498EAC9B471A0D9C87811B5A75E1C3C9FC94D2E2A305406082B069000

APDU>>>>:00B100000454020390FF

APDU<<<<:5381E401050507010304483046300B060604008E46010302010A3037060604008E46010530
2D302B162568747470733A2F2F7777772E72656E6965632E676F622E70652F7265706F7369746F7279
2F13026573308202C60603551D20048202BD308202B930819B06112B060104018293640201030100658
7680030818530 3106082B060105050702011625687474707 33A2F2F7777772E72656E6965632E676F62
2E70652F7265706F7369746F72792F305006082B060105050702023044 1E420050006F006C00ED00740
0690063006100200047006500 6E00650072006100 6C002000640065009000

APDU>>>>:00B100000454020474FF

APDU<<<<:5381E42000430065007200740069006600690063006100630069 00F3006E3081C306112B06
0104018293640201030100678768003081AD303106082B060105050702011625687474707 33A2F2F777
7772E72656E6965632E676F622E70652F7265706F7369746F72792F307806082B060105050702023 06C

1E6A00440650063006C006100720061006300690 0F3006E00200064006500200050007200E10063007
400690063006100730020006400650020004300650072007400690066006900630061006300690 0F3006
E00200045004300450050002D00520045004E0049004500433081AE9000

APDU>>>>:00B100000454020558FF

APDU<<<<:5381E4060604008F7A01023081A33081A006082B06010505070202308193 1E81900050006
F006C00ED00740069006300610020006400650020004300650072007400690066006900630061006400 6
F0020004E006F0072006D0061006C0069007A00610064006F0020004E00430050002B00200064006500
200061006300750065007200640 06F00200063006F006E00200045005400530049002000450 04E002000
330031003900340031003100 1002D00313081A106112B060104018293640201030402678769023081 8B3081
8806082B06010505070202307C1E7A00430065007200740069006900 69000

APDU>>>>:00B10000045402063CFF

APDU<<<<:5381E400690063006100640 06F00200044006900670069007400610 06C0020007000610072
006100200070007200750065006200610073002000430 06C00610073007300200032002000640065002 0
004600690072006D006100200065006E00200068006100720064007700610072006530760603551D1F04
6F306D3034A032A030862E687474703A2F2F63726C2E72656E6965632E676F622E70652F63726C2F7
36861322F6361636C617373322E63726C3035A033A031862F687474703A2F2F63726C322E72656E696
5632E676F622E70652F63726C2F736861322F6361636C617373322E639000

APDU>>>>:00B100000454020720FF

APDU<<<<:5381E4726C300E0603551D0F0101FF040403020640301306035 51D25040C300A06082B06
010505070304302806035 51D110421301F811D70706F72747567616C40706B6965702E72656E6965632
E676F622E7065300D06092A864886F70D01010B0500038202010036CC2C41D80875EDA4C231E58D1
DCC1C53E982062131F1380AF505741DF50C5E5692EB11F9E21B16E06472EB4858525752BF62EBAE
0BDCBEE81DC67A2B22202D7A976A024F92677FD58DED4389BE98D29876EE6379E06EB533AD3AE
C78D89309A1C5B12E292895573D1971387B045D35A86FFDDC2591E5761AE786548119D79000

APDU>>>>:00B100000454020804FF

APDU<<<<:5381E4AEE3062F83407CF946FC95DD407D965CA035D8EB480D093287A5272CCE8CEEF
05604E3AE5916A6435BA5F926914D2125981914B8AD6B3D0A61875B6376C03991C704D91EB3F33A
B241049BA61E8CA34464BEDC9CFEB4A359885E47A34833AA00E460A1564778D80EE41A6F8525672
501CF25C6B2237612B86B188E2316AF96F0886CEA53F3BDE121C9F9974713AA1A1C3CB978A3FF09
984E7F33A1543E2D38BAE2F122F293C4E0978D7F55099AB56579BF4C41A75D8520B637D800D6C2A
70E29FF998C27D99DF9BCCBD21C63169A61F0B8EF8E8D0DDEB3DA6D5068C9A8679FB6A8F854F5
9000

APDU>>>>:00B1000004540208E8FF

APDU<<<<:53819D8BCC2F500A0F69BF5F14B780CE48BB439C4902F067B37FD13499D77736BA23B4
8DBDED9CCE07504C6C1485316F78DBE7012429066FFC0F655EFCDEBA61C014555E26FDA064F362
49469BE0724853A517BEA8CFF9D328CDE614115DA3259FFF80E49AC15297DE87AAF05BAD1C9AD0
60615B6AE04A082A9E059432785AC82ED4DCB91A49654D4B13EE1AC6066F06EEBF4AEC76B00CD
CC569E8798B2374186282