

# General Commands

Secure Element Applet is installed as a non-default applet on a smart card. Before any APDU command is invoked, the applet is selected using the standard Select command.

**NOTE:**  
The availability of specific commands, as well as their content, depends on the secure element (SE) version. You can use the *Get Secure Element Version* command (see below) to check the version of the SE you are using.

## Select Applet

As previously mentioned, the Smart Card has two applets installed. This command selects the Secure Element Applet and routes subsequent APDU commands to it.

### APDU Request

SE Version	IsoCase	Class	Instruction	P1-P2	Command Length (Lc)	Command Data	Expected Length (Le)
>= 2.0.0	Case3Sho	0x00	0xA4	0x040C	0x10	0xA000000748	0x00

### APDU Response

SE Version	Response Data	SW1SW2
>= 2.0.0	none	0x9000

**Example:**

Request: 00A4040010A000000748464A92D546178436F726500

Response: 9000

## Get Secure Element Version

This command returns the version information about the current Api version. The response contains 12 bytes, where each 4 bytes represent unsigned integer of one version segment, making total of 3 version segments: major, minor and patch.

## APDU Request

SE CAP Version	IsoCase	Class	Instruction	P1-P2	Command Length (Lc)	Command Data	Expected Length (Le)
>= 2.0.0	Case2Sho	0x88	0x08	0x000C	none	none	0x00

## APDU Response

SE CAP Version	Response Data	SW1SW2
>= 2.0.0	12 bytes	0x9000

### Example 1:

Request: 8808040000

Response: 000000020000000000000000 9000

### Example 2:

Request: 8808000000

Response: 0000000300000000100000001 9000

### Example 3:

Request: 8808000000

Response: 0000000300000000200000005 9000

## Forward Secure Element Directive

This command is used by E-SDC to forward instructions received from TaxCore.Api to Secure Element Applet via [Secure Element APDU Command](#).

If APDU Command status (SW1SW2) is OK (0x9000), consider forward instructions operation is completed.

**NOTE:**  
From the SE version 3.2.5, optionally, CRC can be calculated and used for data verification. If CRC is not used, the command is the same as in the previous applet version.

# APDU Request

SE Version	IsoCase	Class	Instruction	P1-P2	Command Length (Lc)	Command Data	Expected Length (Le)
>= 2.0.0 (no CRC)	Case3Ext.	0x88	0x40	0x0400	0x000200	512 bytes received from TaxCore	none
>= 3.2.5 (with CRC)	Case3Ext.	0x88	0x40	0x0100	0x000204	512 bytes received from TaxCore + 4 bytes for CRC	none

# APDU Response

SE Version	Response Data	SW1SW2
>= 2.0.0 (no CRC)	none	0x9000
>= 3.2.5 (with CRC)	none	0x9000

## Example 1 (without CRC):

Command Data:  
5DBFC9CD04AF9DC76C50FA3FF54D32D1910B0D2E1EC5AF97EAE3E71A7423CCE066D6E264255838C1DBAD

Request:  
884004000002005DBFC9CD04AF9DC76C50FA3FF54D32D1910B0D2E1EC5AF97EAE3E71A7423CCE066D6E2

Response: 9000

## Example 2 (with CRC):

Command Data without CRC:  
5DBFC9CD04AF9DC76C50FA3FF54D32D1910B0D2E1EC5AF97EAE3E71A7423CCE066D6E264255838C1DBAD

Command Data CRC: F50CFF4B

Command Data:  
5DBFC9CD04AF9DC76C50FA3FF54D32D1910B0D2E1EC5AF97EAE3E71A7423CCE066D6E264255838C1DBAD

Request: 884004000002045DBFC9CD04AF9DC76C50FA3FF54D32D1910B0D2E1EC5AF97EAE3E71A7423CCE066D6E2

Response: 9000

## Export Certificate

This command exports the taxpayer certificate in a DER format. This certificate contains location data that is present on the textual representation of an invoice.

### APDU Request

SE Version	IsoCase	Class	Instruction	P1-P2	Command Length (Lc)	Command Data	Expected Length (Le)
>= 2.0.0	Case2Ext.	0x88	0x04	0x0400	none	none	0x000000

### APDU Response

SE Version	Response Data	SW1SW2
>= 2.0.0	<i>raw bytes random length</i>	0x9000

#### Example:

Request: 88040400000000

Response: *raw bytes of x509 certificate public key* + 9000

## Get Last Signed Invoice

This command returns information about the last signed invoice. The structure of the data received is the same as the response is in the Sign Invoice command.

**NOTE:**  
From the SE version 3.2.5, optionally, CRC can be calculated and used for data verification. If CRC is not used, the command is the same as in the previous applet version.

### APDU Request

SE	IsoCase	Class	Instruction	P1-P2	Command	Command	Expected
----	---------	-------	-------------	-------	---------	---------	----------

Version					Length (Lc)	Data	Length (Le)
>= 3.1.1 (no CRC)	Case2Ext	0x88	0x15	0x0400	none	none	0x000000
>= 3.2.5 (with CRC)	Case2Ext	0x88	0x15	0x0102	none	none	0x000000

## APDU Response

SE Version	Response Data	SW1SW2
>= 3.1.1 (no CRC)	577 or 833 bytes	0x9000
>= 3.2.5 (with CRC)	581 or 837 bytes	0x9000

### Example 1 (without CRC):

Request: 88150400000000

Response: 577 or 833 bytes + 9000

### Response Data

Start (byte)	Length (bytes)	Field	Description
0	8	Date/time	Same as data sent from E-SDC to SE
8	20	Taxpayer ID	Same as data sent from E-SDC to SE
28	20	Buyer ID	Same as data sent from E-SDC to SE
48	1	Invoice type	Same as data sent from E-SDC to SE
49	1	Transaction type	Same as data sent from E-SDC to SE
50	7	Invoice amount	Same as data sent from E-SDC to SE
57	4	Sale or refund counter value	Depends on request's Tax type field
61	4	Total counter value (sale+refund)	Unsigned int 32bit big endian,

65	256 or 512	Encrypted Internal Data	Encrypted Internal Data length depends on the number of available tax rates programmed during personalization. It may be 256 or 512 bytes long.
321 or 577	256	Digital signature	

**Example 2 (with CRC):**

Request: 8815010200

Response: 581 or 837 + 9000

**Response Data**

Start (byte)	Length (bytes)	Field	Description
0	8	Date/time	Same as data sent from E-SDC to SE
8	20	Taxpayer ID	Same as data sent from E-SDC to SE
28	20	Buyer ID	Same as data sent from E-SDC to SE
48	1	Invoice type	Same as data sent from E-SDC to SE
49	1	Transaction type	Same as data sent from E-SDC to SE
50	7	Invoice amount	Same as data sent from E-SDC to SE
57	4	Sale or refund counter value	Depends on request's Tax type field
61	4	Total counter value (sale+refund)	Unsigned int 32bit big endian,
65	256 or 512	Encrypted Internal Data	Encrypted Internal Data length depends on the number of available tax rates programmed during personalization. It may be 256 or 512 bytes long.
321 or 577	256	Digital signature	
577 or 833	4	CRC	CRC is calculated from 0 to 577 or 833 bytes.

# Get PIN tries left from SE Applet

This command returns how many PIN tries are left before the card is locked

## APDU Request

SE Version	IsoCase	Class	Instruction	P1-P2	Command Length (Lc)	Command Data	Expected Length (Le)
>= 3.1.1	Case2Sho	0x00	0x16	0x040C	none	none	0x00

## APDU Response

SE Version	Response Data	SW1SW2
>= 3.1.1	05 if 5 tries are left, 00 if the card is blocked	0x9000

### Example:

Request: 8816040000

Response: 05 9000