Secure Element Applet API

Communication with a Secure element Applet API is performed through standard APDU commands.

For a detailed description of APDU communication, APDU commands data structure and particular bytes meaning, please refer to ISO/IEC 7816-4 standard.

Commands are grouped into three categories based on the type of usage:

1. Fiscalization
2. Audit

Important Notes

1. All APDU commands are sent to the Smart Card using T1 communication protocol
2. All amount values are submitted to the Secure element using Big-endian. Big-endian is an order in which the "big end" (most significant value in the sequence) is stored first (at the lowest storage address)
3. P1 and P2 values are not considered in the request processing, except for the Select Applet Command
4. All APDU commands are sent to the Smart Card using T1 communication protocol
5. All values are submitted to the Secure element using Big-endian. Big-endian is an order in which the "big end" (most significant value in the sequence) is stored first (at the lowest storage address)

Content

1. 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.

2. Fiscalization
   PIN verification is a method that “unlocks” a card for invoice signing and other operations protected by PIN code. PIN is in a decimal format, example PIN:2017 is represented as 0x02, 0x00, 0x01, 0x07

3. Audit
   Returns 259 bytes data structure represents public card key (256 bytes modulus and 3 bytes exponent). This key is used for Audits.

4. Secure Element Specific APDU Error Codes
   This table contains the expected error codes and descriptions that a caller may encounter while working with the Secure Element Applet.

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.

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.

IsoCase: Case4Short

Class: 0x00

Instruction: 0xa4

Data: 0x10 0xA0 0x00 0x00 0x07 0x48 0x46 0x4A 0x49 0x2D 0x54 0x61 0x78 0x43 0x6F 0x72 0x65

Le: 0x00

Example: 0x00 0xA4 0x04 0x00 0x10 0xA0 0x00 0x00 0x07 0x48 0x46 0x4A 0x49 0x2D 0x54 0x61 0x78 0x43 0x6F 0x72 0x65 0x00

Export Certificate

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

IsoCase: Case2Extended

Class: 0x88

Instruction: 0x04

Example: 0x88 0x04 0x04 0x00 0x00 0x00 0x00

Get Secure Element Version

IsoCase: Case2Short

Class: 0x88

Instruction: 0x09

Example: 0x88 0x09 0x04 0x00 0x00

Fiscalization

PIN Verify

PIN verification is a method that “unlocks” a card for invoice signing and other operations protected by PIN code. PIN is in a decimal format, example PIN:2017 is represented as 0x02, 0x00, 0x01, 0x07

IsoCase: Case3Short

Class: 0x88

Instruction: 0x11

Example: 0x88 0x11 0x04 0x00 0x04 0x02 0x00 0x01 0x07 (for Pin 2017)

Sign Invoice

Signs invoice and returns fiscalization data for a submitted invoice.

IsoCase: Case4Extended

Class: 0x88

Instruction: 0x13

Request Data

Start (byte)	Length (byte)	Field	Description
0	8	Date/time	E-SDC timestamp UTC time in Unix Timestamp. Example: 1495018011910 is 2017-05-17T10:46:51.910Z
8	20	Taxpayer ID	Hex encoded byte array, leading bytes filled with 0x00; MSB are sent first Example: Taxpayer ID = 928615467, Byte array = {0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x39, 0x32, 0x38, 0x36, 0x31, 0x35, 0x34, 0x36, 0x37} (byte 0x37 is sent last to SE)
28	20	Buyer ID	If unknown, leave zeroes, formatting is the same as for Taxpayer ID
48	1	Invoice type	Values 0, 1, 2, 3, as explained in section Model

48	1	Invoice type	Values 0, 1, 2, 3, as explained in section Model.
49	1	Transaction Type	Sale=0, Refund=1
50	8	Invoice amount	Sale or refund total amount (including taxes) - depends on applied tax types
58	1	Number of tax categories	Defines the number of tax categories which appear on the invoice (value between 0 and 26). The following data structure **Tax categories** must be repeated exactly this number of times.
77	...		

Tax Categories

Start (byte)	Length (byte)	Field	Description
59	[1]	[Tax category ID]	The first tax category's OrderID, as explained in Tax Rates section (mandatory if **Number of tax categories** > 0)
60	[8]	[Tax category amount]	The first total tax amount for the category specified in preceding field **Tax category ID** (mandatory if **Number of tax categories** > 0)
68	[1]	[Tax category ID]	The next tax category's OrderID (mandatory if **Number of tax categories** > 1)
69	[8]	[Tax category amount]	The next total tax amount for the category specified in preceding field **Tax category ID** (mandatory if **Number of tax categories** > 1)

Request data tables

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	

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	8	Invoice amount	Same as data sent from E-SDC to SE	
58	8	Sale or refund counter value	Depends on request's Tax type field	
66	8	Total counter value (sale+refund)	unsigned int 64bit big endian,	
74	256	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.
330	586	256	Digital signature	
586	842			

Response data table

Example: 0x88 0x13 0x04 0x00 0x00 0x00 0x44 0x00 0x00 0x01 0x5D 0x79 0x40 0x3B 0x69 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x30 0x32 0x31 0x31 0x33 0x31 0x36 0x38 0x32 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x24 0x9F 0x00 0x01 0x03 0x00 0x00 0x00 0x00 0x00 0x02 0x12 0xA9 0x00 0x00

Amount Status

Returns 16 bytes long data structure (8 bytes for sum SALE and REFUND, and 8 bytes for Limit Amount)

IsoCase: Case2Short

Class: 0x88

Instruction: 0x14

Example: 0x88 0x14 0x04 0x00 0x00

Audit

Export TaxCore Public Key

Returns 259 bytes data structure represents public card key (256 bytes modulus and 3 bytes exponent). This key is used for Audits.

IsoCase: Case2Extended

Class: 0x88

Instruction: 0x07

Example: 0x88 0x07 0x04 0x00 0x00 0x00 0x00

Export Internal Data

Exports encrypted Internal Data structure only (256 or 512 bytes).

Class: 0x88

Instruction: 0x12

Example: 0x88 0x12 0x04 0x00 0x00

Start Audit

Notifies the Secure element that the audit process has been initialized by E-SDC.

Secure element returns an encrypted message that shall be submitted to TaxCore as Audit Request Payload.

IsoCase: Case2Extended

Class: 0x88

Instruction: 0x21

Example: 0x88 0x21 0x04 0x00 0x00 0x00 0x00

End Audit

Notifies the Secure element that the audit process has been finalized by TaxCore. If APDU Command status is OK (0x90 0x00) consider audit operation is successfully completed.

IsoCase: Case3Extended

Class: 0x88

Instruction: 0x20

Example: 0x88 0x20 0x04 0x00 0x00 0x01 0x00 0x53 0x8B 0x46 0xC8 0x86 0x48 0x74 0xE4 0x33 0x46 0xA7 0x13 0x81 0x58 0x5E 0xF4 0xD6 0xDC 0xB8 0xB9 0x92 0x42 0x23 0x1B 0xCA 0x60 0xAD 0x41 0x0A 0x70 0x74 0x7B 0xD4 0x8D 0x5F 0xA1 0x21 0x18 0x85 0x07 0x73 0x6B 0x24 0xA3 0x3E 0x4F 0xFE 0x98 0x8C 0x99 0xC2 0x4E 0x77 0x2E 0xF9 0x6F 0xF8 0x72 0x99 0xB8 0x20 0x16 0x2F 0xAD 0xC6 0x97 0xCD 0x42 0xC0 0xA9 0xF1 0x96 0xF8 0x22 0x00 0x7C 0xD4 0xD1 0xE9 0x41 0x19 0x33 0x24 0xF4 0xB0 0x01 0xE1 0x6D 0x40 0xEB 0x9D 0xE1 0xC3 0xBE 0xBE 0x22 0x67 0x4B 0xAC 0xA6 0x23 0x99 0x3F 0xF5 0xA5 0xA2 0x7F 0x67 0x7A 0x01 0x8B 0xC8 0x3E 0x45 0x08 0x7E 0x34 0xCD 0xEA 0x2F 0x0B 0xCF 0x59 0x5F 0xCE 0x9D 0x6B 0xFE 0x36 0x80 0x85 0x86 0x40 0xD3 0xB4 0x3F 0xD7 0x06 0x90 0x79 0x35 0xCE 0x07 0x4B 0x9F 0xAA 0xB8 0x70 0x95 0x5F 0xAC 0x15 0x40 0xE2 0x8A 0x0D 0x5C 0x81 0x27 0x72 0x14 0x00 0xBD 0x68 0x52 0x9B 0x23 0xE5 0xD2 0x23 0x63 0x62 0x87 0x32 0x98 0xA2 0x7A 0x2E 0xDD 0x88 0xD5 0x10 0x0E 0x2B 0x5E 0xA0 0x66 0x89 0xEF 0xD3 0x7E 0x61 0xF9 0x6A 0x6A 0x73 0x4E 0xFE 0xCF 0x6F 0xA6 0xFC 0x67 0xFA 0x88 0xC2 0xA4 0xD5 0x13 0x31 0x12 0x5F 0xC1 0xE8 0x28 0x98 0x87 0x2C 0x43 0xF9 0x11 0x1E 0xC9 0x76 0x16 0xD6 0x9D 0x9D 0x68 0x89 0x7D 0x85 0x0D 0x61 0xB4 0x12 0xB3 0xB5 0x95 0x84 0xCD 0xCA 0x44 0x92 0x9E 0x10 0x22 0x4A 0x10 0x8F 0xB1 0xEE 0xC1 0x1D 0xD4 0xAF

Secure Element Specific APDU Error Codes

This table contains the expected error codes and descriptions that a caller may encounter while working with the Secure Element Applet.

Error Code	Description
0x6301	PIN verification required before executing a command
0x6302	PIN verification failed – wrong PIN code
0x6303	Wrong PIN size
0x6304	Maximum number of tax categories exceeded
0x6305	Maximum amount of tax exceeded (Sign Invoice) or Audit has not been started yet (End Audit)
0x6306	Audit has not started yet
0x6310	The number of allowed PIN entries exceeded
0x63FF	8-byte arithmetic operation overflow

0x6700	Data must be 256 bytes long
0x6A80	Audit Identification is not valid