ISO/IEC JTC 1/SC 17

Date: 2002-01-04

ISO/IEC 7816-3:1997/PDAM-2

ISO/IEC JTC 1/SC 17/WG 4

Secretariat: AFNOR

Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols

AMENDMENT 2: Structures and transmission of APDU messages

Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 3 : Signaux électroniques et protocoles de transmission

AMENDEMENT 2 : Structures et transmission des messages APDU

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

C:\Program Files\Adobe\Acrobat 4.0\Acrobat\plug_ins\OpenAll\Transform\temp\Kyoto3R.doc STD Version 2.0

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this Amendment may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Amendment 2 to International Standard ISO/IEC 7816-3:1997 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Card and personal identification*. During the revision of International Standard ISO/IEC 7816-4:1995, the clause *APDU message structures* and the two annexes *Transportation of APDU messages*, respectively *by T=0* and *by T=1*, have been extracted from the first edition of part 4 for creating this amendment.

ISO/IEC 7816 consists of the following parts, under the general title *Information technology — Identification cards — Integrated circuit(s) cards with contacts*:

— *Part 1: Physical characteristics*

— *Part 2: Dimensions and location of the contacts*

— *Part 3: Electronic signals and transmission protocols*

— *Part 4: Interindustry commands for interchange*

— *Part 5: Numbering system and registration procedure for application identifiers*

— *Part 6: Interindustry data elements for interchange*

— *Part 7: Interindustry commands for Structured Card Query Language (SCQL)*

— *Part 8: Interindustry commands for a cryptographic toolbox*

— *Part 9: Interindustry commands for card and file management*

— *Part 10: Electronic signals and answer to reset for synchronous cards*

— *Part 11: Personal verification through biometric methods*

— *Part 15: Cryptographic information application*

Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols

AMENDMENT 2: Structures and transmission of APDU messages

Insert the following three clauses.

10 Application protocol data units

A step in an application protocol consists of sending a command, processing it in the receiving entity and returning the response.

Therefore a specific response corresponds to a specific command, referred to as a command-response pair. ISO/IEC 7816 supports only command-response pairs that shall be completed before initiating a subsequent command-response pair.

An application protocol data unit (APDU) is either a command message or a response message, sent from the interface device to the card or conversely.

10.1 Command APDU

Illustrated by Figure 23, each command APDU defined in this part of ISO/IEC 7816 consists of

— a mandatory header of four bytes denoted as CLA-INS-P1-P2,

— a conditional body of variable length.

Command header	Command body
CLA - INS - P1 - P2	[Lc field] - [Data field] - [Le field]

Figure 23 — Command APDU structure

Number Lc (length of command data) is the number of bytes present in the data field of the command APDU. If number Lc is zero, then both the Lc field and the data field are absent.

Number Le (length of expected data) is the maximum number of bytes expected in the data field of the response APDU. If number Le is zero, then the Le field is absent. If the Le field contains only bytes set to '00', then the maximum number of available data bytes is requested.

10.2 Response APDU

Illustrated by Figure 24, each response APDU defined in this part of ISO/IEC 7816 consists of

— a conditional body of variable length,

— a mandatory trailer of two bytes denoted as SW1-SW2.

Response body	Response trailer
[Data field]	SW1 - SW2

Figure 24 — Response APDU structure

Number Lr (length of response data) is the number of bytes present in the data field of the response APDU. If the data field is absent, then number Lr is zero. Number Lr shall be in the range zero to number Le.

The trailer codes the status of the receiving entity after processing the command-response pair.

NOTE If the command is aborted, then the response APDU is a trailer coding an error condition on two status bytes.

10.3 Data fields and length fields

In a command-response pair, the command APDU and the response APDU may contain a data field, thus inducing the four cases summarized by table 13.

Table 13 — Data fields within a command-response pair

Case	Command APDU	Response APDU
1	No data field	No data field
2	No data field	Data field
3	Data field	No data field
4	Data field	Data field

In case 1, as both numbers Lc and Le are zeroes, the command APDU consists of one field, namely the command header. The command body is absent: the Lc field, the data field and the Le field are absent.

In case 2, as number Lc is zero and number Le is not zero, the command APDU consists of two successive fields, namely the command header and the Le field. The Lc field and the data field are absent.

In case 3, as number Lc is not zero and number Le is zero, the command APDU consists of three successive fields, namely the command header, the Lc field and the data field. The Le field is absent.

In case 4, as both numbers Lc and Le are not zeroes, the command APDU consists of four successive fields, namely the command header, the Lc field, the data field and the Le field.

Figure 25 shows the four structures of command APDUs according to the previous four cases.

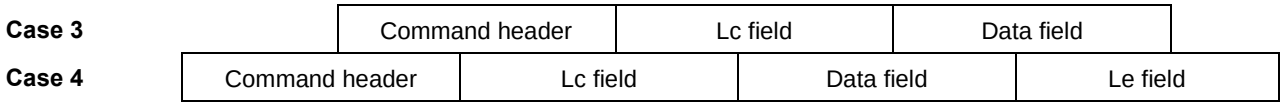


Figure 25 — The four structures of command APDUs

A command APDU carries no length field in case 1, one length field in cases 2 and 3, two length fields in case 4.

In the historical bytes of the Answer-to-Reset, the card states whether the Lc and Le fields shall be short (default value) or may be extended (explicit statement, see card capabilities in ISO/IEC 7816-4).

Figure 26 illustrates a command APDU as a string of L bytes (at least four bytes) denoted from C(1) to C(L); the first four bytes are the command header, namely CLA-INS-P1-P2.

{C(1) = CLA} - {C(2) = INS} - {C(3) = P1} - {C(4) = P2} - [C(5)] - … [C(L)]

Figure 26 — Command APDU as a byte string

The cases 2, 3 and 4 are either short or extended.

— In the short cases abbreviated as cases 2S, 3S and 4S, there is one byte for each length field, namely byte C(5) in cases 2S and 3S, byte C(5) and byte C(L) in case 4S.

— In the extended cases abbreviated as cases 2E, 3E and 4E, byte C(5) is set to '00': it is part of the first length field and there are two other bytes for each length field, namely bytes C(6)-C(7) in cases 2E and 3E, bytes C(6)-C(7) and bytes C(L–1)-C(L) in case 4E.

10.4 Decoding conventions for command APDUs

Table 14 shows the command APDU decoding according to the previous seven cases.

Table 14 — Command APDU decoding

Conditions			Case
L = 4	-	-	1
L = 5	-	-	Short 2 (2S)
L = 5 + (C(5))	C(5) is not '00'	-	Short 3 (3S)
L = 6 + (C(5))	C(5) is not '00'	-	Short 4 (4S)
L = 7	C(5) is '00'	-	Extended 2 (2E)
L = 7 + (C(6)-C(7))	C(5) is '00'	C(6)-C(7) is not '0000'	Extended 3 (3E)
L = 9 + (C(6)-C(7))	C(5) is '00'	C(6)-C(7) is not '0000'	Extended 4 (4E)
Any other command APDU is invalid.			

The first four cases apply to all cards.

Case 1 — L = 4 — No byte is used for numbers Lc and Le, both equal to zero. The command body is absent.

Case 2S — L = 5 — No byte is used for number Lc equal to zero. The Le field consists of byte C(5); it codes number Le in the range from 1 to 256 (byte C(5) set to '00' means maximum, i.e., number Le equal to 256).

Case 3S — L = 5 + (C(5)) where C(5) is not set to '00' — The Lc field consists of byte C(5); it codes number Lc in the range from 1 to 255. The data field consists of the subsequent Lc bytes from C(6) to C(L). No byte is used for number Le equal to zero.

Case 4S — L = 6 + (C(5)) where C(5) is not set to '00' — The Lc field consists of byte C(5); it codes number Lc in the range from 1 to 255. The data field consists of the subsequent Lc bytes from C(6) to C(L–1). The Le field consists of byte C(L); it codes number Le in the range from 1 to 256 (byte C(L) set to '00' means maximum, i.e., number Le equal to 256).

For cards indicating the extension of Lc and Le fields (see card capabilities in ISO/IEC 7816-4), the next three cases also apply.

Case 2E — L = 7 where C(5) is set to '00' — No byte is used for number Lc equal to zero. The Le field consists of bytes C(5)-C(6)-C(7); bytes C(6)-C(7) code number Le in the range from 1 to 65 536 (bytes C(6)-C(7) set to '0000' means maximum, i.e., number Le equal to 65 536).

Case 3E — L = 7 + (C(6)-C(7)) where C(5) is set to '00' and C(6)-C(7) not set to '0000' — The Lc field consists of bytes C(5)-C(6)-C(7); bytes C(6)-C(7) code number Lc in the range from 1 to 65 535. The data field consists of the subsequent Lc bytes from C(8) to C(L). No byte is used for number Le equal to zero.

Case 4E — L = 9 + (C(6)-C(7)) where C(5) is set to '00' and C(6)-C(7) not set to '0000' — The Lc field consists of bytes C(5)-C(6)-C(7); bytes C(6)-C(7) code number Lc in the range from 1 to 65 535. The data field consists of the subsequent Lc bytes from C(8) to C(L–2). The Le field consists of bytes C(L–1)-C(L); they code number Le in the range from 1 to 65 536 (bytes C(L–1)-C(L) set to '0000' means maximum, i.e., number Le equal to 65 536).

11 Command-response pair transmission by T=0

11.1 Case 1

The command APDU is mapped onto the command TPDU by setting byte P3 to '00'.

Command APDU	CLA - INS - P1 - P2
Command TPDU	CLA - INS - P1 - P2 - {P3 set to '00'}

The response TPDU is mapped onto the response APDU without any change.

Response TPDU	SW1 - SW2
Response APDU	SW1 - SW2

11.2 Case 2 Short

In this case, the Le field consists of byte C(5); it codes number Le in the range from 1 to 256 (C(5) set to '00' means maximum, i.e., number Le equal to 256). The command APDU is mapped onto the command TPDU without any change.

Command APDU	CLA - INS - P1 - P2	{Le field = C(5)}
Command TPDU	CLA - INS - P1 - P2 - {P3 = C(5)}	

The response TPDU is mapped onto the response APDU according to the acceptance of number Le and according to the processing of the command.

Case 2S.1 — Le accepted

The response TPDU is mapped onto the response APDU without any change.

Response TPDU	Le data bytes	SW1 - SW2
Response APDU	Le data bytes	SW1 - SW2

Case 2S.2 — Le definitely not accepted

The card does not accept number Le; it does not support the service of providing data if the length is wrong. The response TPDU from the card indicates that the card aborts the command due to a wrong length: SW1 set to '67'. The response TPDU is mapped onto the response APDU without any change.

Response TPDU	{SW1 set to '67'} - SW2
Response APDU	{SW1 set to '67'} - SW2

Case 2S.3 — Le not accepted, La indicated

The card does not accept number Le and the response TPDU from the card indicates that the command is aborted due to a wrong length and that La data bytes are available: SW1 set to '6C' and SW2 codes number La.

Response TPDU	{SW1 set to '6C'} - SW2

— If the transmission system does not support the service of re-issuing the same command, it shall map the response TPDU onto the response APDU without any change.

Response APDU	{SW1 set to '6C'} - SW2

— If the transmission system supports the service of re-issuing the same command, it shall re-issue the same command TPDU by setting byte P3 to byte SW2.

Command TPDU	CLA - INS - P1 - P2 - {P3 = SW2}

The response TPDU consists of La bytes followed by two status bytes SW1-SW2.

Response TPDU	La data bytes	SW1 - SW2

- If La ≤ Le, then the response TPDU is mapped onto the response APDU without any change.

Response APDU	La data bytes	SW1 - SW2

- If La is more than Le, then the response TPDU is mapped onto the response APDU by keeping only the first Le bytes of the response APDU and the two status bytes SW1-SW2.

Response APDU	Le (less than La) data bytes	SW1 - SW2

Case 2S.4 — SW1-SW2 set to '9XYZ', except for '9000'

The response TPDU is mapped onto the response APDU without any change.

11.3 Case 3 Short

In this case, the Lc field consists of byte C(5) not set to '00'; it codes number Lc in the range from 1 to 255. The command APDU is mapped onto the command TPDU without any change.

Command APDU	CLA - INS - P1 - P2	{Lc field = C(5)}	Lc data bytes
Command TPDU	CLA - INS - P1 - P2 - {P3 = C(5)}		Lc data bytes

The response TPDU is mapped onto the response APDU without any change.

Response TPDU	SW1 - SW2
Response APDU	SW1 - SW2

11.4 Case 4 Short

In this case, the Lc field consists of byte C(5) not set to '00'; it codes number Lc in the range from 1 to 255; the Le field consists of byte C(L); it codes number Le in the range from 1 to 256 (C(L) set to '00' means maximum i.e., number Le equal to 256). The command APDU is mapped onto the command TPDU by cutting off the Le field, i.e., C(L).

Command APDU	CLA - INS - P1 - P2	{Lc field = C(5)}	Lc data bytes	{Le field = C(L)}
Command TPDU	CLA - INS - P1 - P2 - {P3 = C(5)}		Lc data bytes	

Case 4S.1 — Command not accepted

The first response TPDU from the card indicates that the card aborted the command: SW1 set to '6X', except for '61', '62' and '63'. The response TPDU is mapped onto the response APDU without any change.

Response TPDU	{SW1 set to '6X' except for '61', '62' and '63'} - SW2
Response APDU	{SW1 set to '6X' except for '61', '62' and '63'} - SW2

Case 4S.2 — Command accepted

The first response TPDU from the card indicates that the card performed the command: SW1-SW2 set to '9000', '62XX' or '63XX'. The transmission system shall issue a GET RESPONSE command TPDU to the card by setting byte P3 to byte C(L) coding number Le.

Command TPDU	CLA - {INS = GET RESPONSE} - P1 - P2 - {P3 = C(L)}

Depending on the second response TPDU from the card, the transmission system shall react as described in cases 2S.1, 2S.2, 2S.3 and 2S.4 above.

Case 4S.3 — Command accepted with information added

The first response TPDU from the card indicates that the card performed the command and gives information on the number of available data bytes: SW1 set to '61' and byte SW2 codes number Lx. The transmission system shall issue a GET RESPONSE command TPDU to the card by setting byte P3 to the minimum of numbers Lx and Le.

Command TPDU	CLA - {INS = GET RESPONSE} - P1 - P2 - {P3 = min(Le, Lx)}

The second response TPDU is mapped onto the response APDU without any change.

Response TPDU	P3 data bytes	SW1 - SW2
Response APDU	P3 data bytes	SW1 - SW2

Case 4S.4 — SW1-SW2 set to '9XYZ', except for '9000'

The response TPDU is mapped onto the response APDU without any change.

11.5 Case 2 Extended

In this case, the Le field consists of bytes C(5)-C(6)-C(7); C(5) set to '00'; C(6)-C(7) code number Le in the range from 1 to 65 536 (C(6)-C(7) set to '0000' means maximum, i.e., number Le equal to 65 536).

Command APDU	CLA - INS - P1 - P2	{Le field = C(5)-C(6)-C(7)}

Case 2E.1 — Le ≤ 256, C(5) set to '00', C(6)-C(7) from '0001' to '0100'

The command APDU shall be mapped onto the command TPDU by setting byte P3 to byte C(7) coding number Le in the range from 1 to 256. The processing by the transmission system shall be according to case 2S.

Command TPDU	CLA - INS - P1 - P2 - {P3 = C(7)}

Case 2E.2 — Le more than 256, C(5) set to '00', C(6)-C(7) either set to '0000' or from '0101' to 'FFFF'

The command APDU shall be mapped onto the command TPDU by setting byte P3 to '00'.

Command TPDU	CLA - INS - P1 - P2 - {P3 set to '00'}

a) If the first response TPDU from the card indicates that the card aborted the command due to a wrong length (SW1 set to '67'), then the response TPDU shall be mapped onto the response APDU without any change.

Response TPDU	{SW1 set to '67'} - SW2
Response APDU	{SW1 set to '67'} - SW2

b) If the first response TPDU from the card indicates that the command is aborted due to a wrong length and that La data bytes are available, i.e., SW1 set to '6C' and (SW2) equal to La, then the transmission system shall complete the processing as described in case 2S.3.

c) If the first response TPDU is 256 data bytes followed by SW1-SW2 set to '9000', this means that the card has no more than 256 data bytes, and/or does not support the GET RESPONSE command. The transmission system shall then map the response TPDU onto the response APDU without any change.

Response TPDU	256 data bytes	{SW1 - SW2 set to '9000'}
Response APDU	256 data bytes	{SW1 - SW2 set to '9000'}

d) If the first or subsequent response TPDU from the card is SW1 set to '61', then SW2 codes number Lx, i.e., the number of extra bytes available from the card (SW2 set to '00' indicates 256 bytes or more), the transmission system shall compute number Lm, i.e., number Le minus the number of data bytes received in the previous response TPDU(s), so as to obtain the number of remaining data bytes to be retrieved from the card.

- If Lm is zero, then the transmission system shall concatenate the bodies of all received response TPDUs together with the trailer of the last received response TPDU into the response APDU.
- If Lm is positive, then the transmission system shall issue a GET RESPONSE command TPDU by setting byte P3 to the minimum of Lx and Lm. The corresponding response TPDU from the card shall be processed
  - — according to case d), if SW1 is set to '61',
  - — as above when Lm is zero, if SW1 is set to '90'.

11.6 Case 3 Extended

In this case, the Lc field consists of bytes C(5)-C(6)-C(7) where C(5) is set to '00' and C(6)-C(7) not set to '0000'; bytes C(6)-C(7) code number Lc in the range from 1 to 65 535.

Command APDU	CLA - INS - P1 - P2	{Lc field = C(5)-C(6)-C(7)}	Lc data bytes

Case 3E.1 — Lc from one to 255, C(5)-C(6) set to '0000', C(7) is not set to '00'

In this case, byte C(7) codes number Lc in the range from 1 to 255. The command APDU is mapped onto the command TPDU by setting byte P3 to byte C(7).

Command TPDU	CLA - INS - P1 - P2 - {P3 = C(7)}	Lc data bytes

The response TPDU is mapped onto the response APDU without any change.

Response TPDU	SW1 - SW2
Response APDU	SW1 - SW2

Case 3E.2 — Lc more than 255, C(5) set to '00', C(6) not set to '00', C(7) any value

— If the transmission system does not support the ENVELOPE command, it shall return an error response APDU meaning that the length is wrong: SW1 set to '67'.

Response TPDU	{SW1 set to '67'} - SW2
Response APDU	{SW1 set to '67'} - SW2

— If the transmission system supports the ENVELOPE command, it shall split the APDU into segments of length less than 256 bytes, and send those successive segments into the bodies of consecutive ENVELOPE command TPDUs.

Command TPDU	CLA - {INS = ENVELOPE} - P1 - P2 - P3	P3 bytes

o If the first response TPDU from the card indicates that the card does not support the ENVELOPE command (SW1 set to '6D'), the TPDU shall be mapped onto the response TPDU without any change.

Response TPDU	{SW1 set to '6D'} - SW2
Response APDU	{SW1 set to '6D'} - SW2

o If the first response TPDU from the card indicates that the card does support the ENVELOPE command (SW1-SW2 set to '9000'), the transmission system shall send further ENVELOPE commands as needed.

Response TPDU	{SW1 - SW2 set to '9000'}	
Command TPDU	CLA - {INS = ENVELOPE} - P1 - P2 - P3	P3 bytes

o The response TPDU corresponding to the last ENVELOPE command is mapped onto the response APDU without any change.

Response TPDU	SW1 - SW2
Response APDU	SW1 - SW2

11.7 Case 4 Extended

In this case, the Lc field consists of bytes C(5)-C(6)-C(7) where C(5) is set to '00' and C(6)-C(7) not set to '0000'; bytes C(6)-C(7) code number Lc in the range from 1 to 65 535; the Le field consists of bytes C(L–1)-C(L); they code number Le in the range from 1 to 65 536 (C(L–1)-C(L) set to '0000' means maximum, i.e., number Le equal to 65 536).

Command APDU	CLA - INS - P1 - P2	{Lc field = C(5)-C(6)-C(7)}	Lc data bytes	{Le field = C(L–1)-C(L)}

Case 4E.1 — Lc less than 256, C(5)-C(6) set to '0000', C(7) not set to '00'

In this case, byte C(7) codes number Lc in the range from 1 to 255. The command APDU is mapped onto the command TPDU by setting byte P3 to byte C(7) and by appending the Lc data bytes. The Le field, i.e., C(L–1)-C(L), is cut off.

Command TPDU	CLA - INS - P1 - P2 - {P3 = C(7)}	Lc data bytes

a) If SW1 is set to '6X' except for '61', '62' or '63' in the first response TPDU from the card, then the response TPDU is mapped onto the response APDU without any change.

Response TPDU	{SW1 set to '6X' except for '61', '62' or '63'} - SW2
Response APDU	{SW1 set to '6X' except for '61', '62' or '63'} - SW2

b) If SW1 is set to '90', '62' or '63' in the first response TPDU from the card, then

- If Le is 256 or less, i.e., C(L–1)-C(L) in the range from '0001' to '0100', then the transmission system shall issue a GET RESPONSE command TPDU by setting byte P3 to byte C(L). The subsequent processing by the transmission system shall be according to cases 2S.1, 2S.2, 2S.3 and 2S.4 above.
- If Le is more than 256, i.e., C(L–1)-C(L) either set to '0000' or greater than '0100', then the transmission system shall issue a GET RESPONSE command TPDU by setting byte P3 to '00'. The subsequent processing by the transmission system shall be according to case 2E.2 above.

c) If SW1 is set to '61' in the first response TPDU from the card, then the transmission system shall proceed as specified in case 2E.2 d) above.

Case 4E.2 — Lc more than 255, C(5) set to '00', C(6) not set to '00', C(7) any value

The transmission system shall go on according to case 3E.2 described above, until the command APDU has been sent completely to the card. It shall then go on as described in case 4E.1 a), b) and c) described above.

12 Command-response pair transmission by T=1

12.1 Case 1

The command APDU is mapped onto the information field of an I-block without any change.

Command APDU	CLA - INS - P1 - P2
Information field	CLA - INS - P1 - P2

The information field of the I-block received in response is mapped onto the response APDU without any change.

Information field	SW1 - SW2
Response APDU	SW1 - SW2

12.2 Case 2 (short and extended)

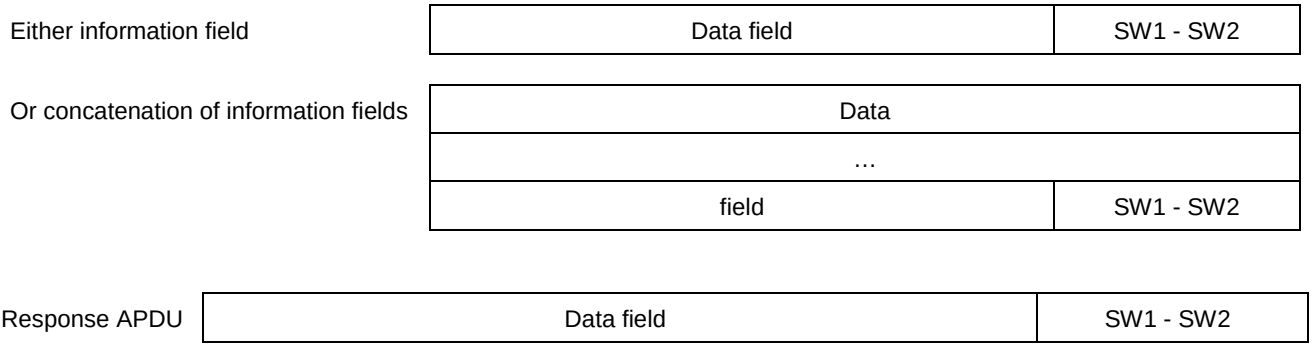
The command APDU is mapped onto the information field of an I-block without any change.

Command APDU	CLA - INS - P1 - P2	Le field
Information field	CLA - INS - P1 - P2	Le field

The response APDU consists of

— either the information field of the I-block received in response,

— or the concatenation of the information fields of successive I-blocks received in response. These blocks shall be chained.

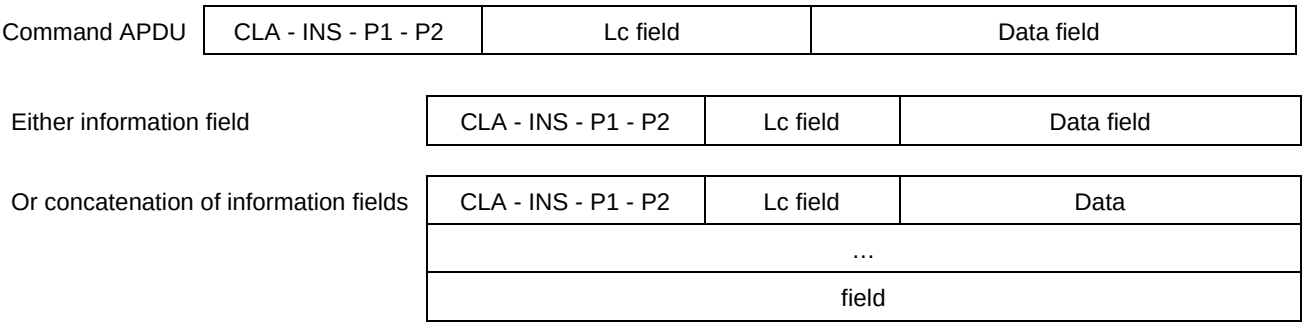


12.3 Case 3 (short and extended)

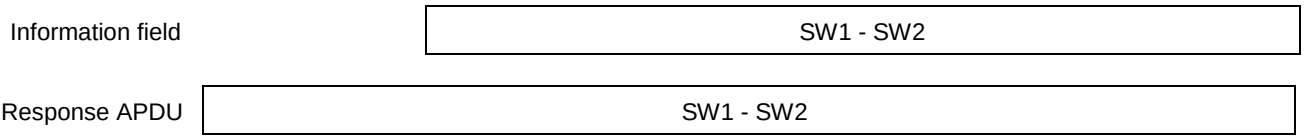
The command APDU is mapped without any change onto

— either the information field of one I-block,

— or the concatenation of the information fields of successive I-blocks. These blocks shall be chained.



The information field of the I-block received in response is mapped onto the response APDU without any change.

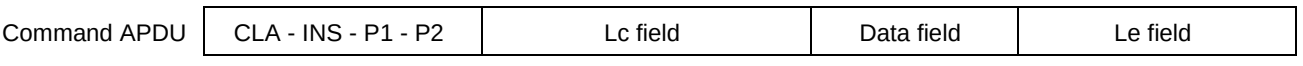


12.4 Case 4 (short and extended)

The command APDU is mapped without any change onto

— either the information field of one I-block,

— or the concatenation of the information fields of successive I-blocks. These blocks shall be chained.



Either information field	CLA - INS - P1 - P2	Lc field	Data field	Le field

Or concatenation of information fields	CLA - INS - P1 - P2	Lc field	Data
	…		
	field		Le field

The response APDU consists of

— either the information field of the I-block received in response,

— or the concatenation of the information fields of successive I-blocks received in response. These blocks shall be chained.

Either information field	Data field	SW1 - SW2

Or concatenation of information fields	Data	
	…	
	field	SW1 - SW2

Response APDU	Data field	SW1 - SW2