INTERNATIONAL STANDARD

ISO/IEC 7816-4

First edition
1995-09-01

AMENDMENT 1
1997-12-15

Information technology — Identification cards — Integrated circuit(s) cards with contacts —

Part 4: Interindustry commands for interchange

AMENDMENT 1: Impact of secure messaging on the structures of APDU messages

Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts —

Partie 4: Commandes intersectorielles pour les échanges

AMENDEMENT 1: Impact de la messagerie de sécurité sur les structures des messages APDU

Reference number
ISO/IEC 7816-4:1995/Amd.1:1997(E)

Contents

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.

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.

Amendment 1 to International Standard ISO/IEC 7816-4:1995 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Identification cards and related devices*.

Introduction

The integrated circuit(s) cards with contacts are identification cards intended for information exchange negotiated between the outside and the integrated circuit in the card. As a result of an information exchange, the card delivers information (computation results, stored data), and/or modifies its content (data storage, event memorization).

Part 4 of ISO/IEC 7816 is one of a series of standards describing the parameters for such cards and the use of such cards for international interchange.

This amendment fixes the impact of secure messaging on the structures of APDU messages.

Information technology — Identification cards — Integrated circuit(s) cards with contacts —

Part 4:
Interindustry commands for interchange

AMENDMENT 1: Impact of secure messaging on the structures of APDU messages

In table 19, replace the last line by the following two lines.

'96', '97'	— Value of L_e in the unsecured command
'99'	— Status information (e.g., SW1 SW2)

In table 21, replace the value 'BA' by the following two values.

'AC', 'BC'

Insert the following subclause.

5.7 Impact of secure messaging on the structures of APDU messages

The structures of APDU messages are specified in 5.3. According to 5.3.1, the command APDU consists of a mandatory command header of four bytes conditionally followed by a command body (see figures 3 and 4); the decoding of the command body is specified in 5.3.2 (see figure 5 and table 5). According to 5.3.3, the response APDU consists of a conditional response body followed by a mandatory response trailer of two bytes (see figure 6). Figure 8 shows the structures of APDU messages.

Command header	Command body
CLA INS P1 P2 (four bytes)	[L_c field] [Data field] [L_e field] (L bytes, denoted as B_1 to B_L)

Response body	Response trailer
[Data field] (L_r data bytes)	SW1 SW2 (two bytes)

Figure 8 — Structures of APDU messages

Clause 6 specifies APDU commands and responses for basic interindustry commands. Clause 7 specifies APDU commands and responses for transmission-oriented interindustry commands. Clauses 6 and 7 do not describe the impact of secure messaging (see 5.6) on the structures of APDU messages. Consequently, the semantic meanings of length fields and data fields in clauses 6 and 7 may seem in contradiction with their syntactic meanings in 5.3.

This subclause specifies the impact of secure messaging as specified in 5.6 on the structures of APDU messages as specified in 5.3, so as to avoid the aforementioned possible misunderstanding.

For securing an APDU command where CLA has an appropriate value according to table 9, namely '0X', '8X', '9X' or 'AX', the bit b4 in CLA shall be set to 1, which is indicated as CLA* in figure 9 and annex F; if present, the command body shall be decoded according to 5.3.2 and encapsulated as follows.

— If there is a data field, the L_c data bytes shall be carried

- either by a plain value data object ('80', '81', 'B2', 'B3', see table 19),
- or by a data object for confidentiality (from '84' to '87', see table 22).

— If there is an L_e field, the value of L_e shall be carried by a L_e data object (either '96' or '97', see table 19); the value field codes an unsigned positive integer on one or two bytes; both the null value and the empty data object mean the maximum.

Similarly, the response APDU shall be encapsulated as follows.

— If there is a data field, the L_r data bytes shall be carried

- either by a plain value data object ('80', '81', 'B2', 'B3', see table 19),
- or by a data object for confidentiality (from '84' to '87', see table 22).

— If needed, the response trailer shall be carried by a status information data object ('99', see table 19); the empty data object means SW1 SW2 = '9000'.

Figure 9 shows the structures of secured APDU messages.

— Every new data field may carry additional SM data objects, e.g., a cryptographic checksum ('8E') at the end. Annex F provides illustrative examples.

— The new L_c field gives the length of the new data field of the secured command APDU.

— The new L_e field shall be empty when no data field is expected in the secured response APDU; otherwise, it shall contain only zeroes.

— The new response trailer codes the status of the receiving entity after processing the secured command. It may be encapsulated for protection.

Command header	Command body
CLA* INS P1 P2 (four bytes)	[New L_c field] { [New data field] = [T L_c Data bytes] [T '01' or '02' L_e] } [New L_e field]

Response body	Response trailer
[New data field] = [T L_r Data bytes] [T '02' New SW1 SW2]	New SW1 SW2 (two bytes)

Figure 9 — Structures of secured APDU messages

NOTES

1 The lengths from 1 to 127 are coded in the same way in BER-TLV length fields as in APDU length fields. The codings differ for 128 and more.

2 As stated above, further or other SM data objects may be present in the new data fields.

3 When securing messages, it is not always apparent whether the data to be protected have a BER-TLV structure. Then the tags '80', '81', '86' and '87' are recommended.

Replace the existing annex F (two pages) by the following revision (three pages).

Annex F

(informative)

Use of secure messaging

F.1 Abbreviations

For the purposes of this annex, the following abbreviations apply.

CC cryptographic checksum
CG cryptogram
CH command header (CLA INS P1 P2)
CR control reference
FR file reference
KR key reference
L length
LE value of L_e in the unsecured command (one or two bytes coding an unsigned positive integer; the null value means the maximum)
PB padding bytes ('80' followed by 0 to k-1 times '00' where k is the block length)
PI padding indicator byte
PV plain value
RD response descriptor
T tag
|| concatenation

F.2 Cryptographic checksum

According to 5.7, the use of cryptographic checksums (see 5.6.3.1) is shown for the four cases defined in table 4 and figure 4. In the examples, the value of L_{CC} is four. CLA* indicates the use of secure messaging, i.e., the bit b4 is equal to 1 in CLA which is equal to '0X', '8X', '9X' or 'AX' according to table 9.

— Case 1 — No data, no data

The unsecured command-response pair is as follows.

Command header	Command body
CLA INS P1 P2	Empty

Response body	Response trailer
Empty	SW1 SW2

— Case 1.a — Status not to be protected

The secured command APDU is as follows.

Command header	Command body
CLA* INS P1 P2	New L_c field (one byte = '06') || New data field (six bytes)

New data field = One data object = T_{CC} || L_{CC} || CC

Data covered by CC (b3=1 in CLA*) = One block = CH || PB

The secured response APDU is as follows.

Response body	Response trailer
Empty	New SW1 SW2

— Case 1.b — Status to be protected

The secured command APDU is as follows.

Command header	Command body
CLA* INS P1 P2	New L_c field (one byte ='06') || New data field (six bytes) || New L_e field (one byte = '00')

New data field = One data object = T_{CC} || L_{CC} || CC

Data covered by CC (b3=1 in CLA*) = One block = CH || PB

The secured response APDU is as follows.

Response body	Response trailer
New data field	New SW1 SW2

New data field = Two data objects = T_{SW} (b1=1) || L_{SW} || SW (= New SW1 SW2) || T_{CC} || L_{CC} || CC

Data covered by CC = One block = T_{SW} (b1=1) || L_{SW} || SW || PB

— Case 2 — No data, data

The unsecured command-response pair is as follows.

Command header	Command body
CLA INS P1 P2	L_e field

Response body	Response trailer
Data field	SW1 SW2

The secured command APDU is as follows.

Command header	body
CLA* INS P1 P2	New L_c field ‖ New data field ‖ New L_e field (one or two bytes = '00')

New data field = Two data objects =
T_{LE} (b1=1) ‖ L_{LE} ‖ LE ‖
T_{CC} ‖ L_{CC} ‖ CC

Data covered by CC =
- One block if b3=0 in CLA* =
  T_{LE} (b1=1) ‖ L_{LE} ‖ LE ‖ PB
- Two blocks if b3=1 in CLA* =
  CH ‖ PB ‖
  T_{LE} (b1=1) ‖ L_{LE} ‖ LE ‖ PB

The secured response APDU is as follows.

Response body	Response trailer
New data field	New SW1 SW2

New data field = Three data objects =
T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖
[T_{SW} (b1=1) ‖ L_{SW} ‖ SW (= New SW1 SW2)] ‖
T_{CC} ‖ L_{CC} ‖ CC

Data covered by CC = One or more blocks =
T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖ [T_{SW} (b1=1) ‖ L_{SW} ‖ SW] ‖ PB

— Case 3 — Data, no data

The unsecured command-response pair is as follows.

Command header	Command body
CLA INS P1 P2	L_c field ‖ Data field

Response body	Response trailer
Empty	SW1 SW2

— Case 3.a — Status not to be protected

The secured command APDU is as follows.

Command header	Command body
CLA* INS P1 P2	New L_c field ‖ New data field

New data field = Two data objects =
T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖
T_{CC} ‖ L_{CC} ‖ CC

Data covered by CC =
- One or more blocks if b3=0 in CLA* =
  T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖ PB
- Two or more blocks if b3=1 in CLA* =
  CH ‖ PB ‖
  T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖ PB

The secured response APDU is as follows.

Response body	Response trailer
Empty	New SW1 SW2

— Case 3.b — Status to be protected

The secured command APDU is as follows.

Command header	Command body
CLA* INS P1 P2	New L_c field ‖ New data field ‖ New L_e field (one or two bytes = '00')

New data field = Two data objects =
T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖
T_{CC} ‖ L_{CC} ‖ CC

Data covered by CC =
- One or more blocks if b3=0 in CLA* =
  T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖ PB
- Two or more blocks if b3=1 in CLA* =
  CH ‖ PB ‖
  T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖ PB

The secured response APDU is as follows.

Response body	Response trailer
New data field	New SW1 SW2

New data field = Two data objects =
T_{SW} (b1=1) ‖ L_{SW} ‖ SW (= New SW1 SW2) ‖
T_{CC} ‖ L_{CC} ‖ CC

Data covered by CC = One block =
T_{SW} (b1=1) ‖ L_{SW} ‖ SW ‖ PB

— Case 4 — Data, data

The unsecured command-response pair is as follows.

Command header	Command body
CLA INS P1 P2	L_c field ‖ Data field ‖ L_e field

Response body	Response trailer
Data field	SW1 SW2

The secured command APDU is as follows.

Command header	Command body
CLA* INS P1 P2	New L_c field ‖ New data field ‖ New L_e field (one or two bytes = '00')

New data field = Three data objects =
T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖
T_{LE} (b1=1) ‖ L_{LE} ‖ LE ‖
T_{CC} ‖ L_{CC} ‖ CC

Data covered by CC =
- One or more blocks if b3=0 in CLA* =
  T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖ T_{LE} (b1=1) ‖ L_{LE} ‖ LE ‖ PB
- Two or more blocks if b3=1 in CLA* =
  CH ‖ PB ‖
  T_{PV} (b1=1) ‖ L_{PV} ‖ PV ‖ T_{LE} (b1=1) ‖ L_{LE} ‖ LE ‖ PB

The secured response APDU is as follows.

Response body	Response trailer
New data field	New SW1 SW2

New data field = Three data objects =
T_{PV} (b1=1) || L_{PV} || PV ||
[T_{SW} (b1=1) || L_{SW} || SW (= New SW1 SW2)] ||
T_{CC} || L_{CC} || CC

Data covered by CC = One or more blocks =
T_{PV} (b1=1) || L_{PV} || PV || [T_{SW} (b1=1) || L_{SW} || SW] || PB

F.3 Cryptograms

The use of cryptograms with and without padding (see 5.6.4) is shown in data fields (command APDU as well as response APDU). Instead of the plain value data objects in the previous examples, data objects for confidentiality shall be used as follows.

— Case a — Plain data not coded in BER-TLV

Data field =
$T_{PI\ CG}$ || $L_{PI\ CG}$ || PI || CG

Data carried by CG = One or more blocks =
Non BER-TLV coded data
and padding bytes according to PI

— Case b — Plain data coded in BER-TLV

Data field =
T_{CG} || L_{CG} || CG

Data carried by CG = String of concealed bytes =
BER-TLV data objects (padding depending on the algorithm and its mode of operation)

F.4 Control references

The use of control references (see 5.6.5.1) is shown.

Command data field =
T_{CR} || L_{CR} || CR
where CR = T_{FR} || L_{FR} || FR || T_{KR} || L_{KR} || KR

F.5 Response descriptor

The use of response descriptors (see 5.6.5.2) is shown.

Command data field =
T_{RD} || L_{RD} || RD
where RD = T_{PV} || '00' || T_{CC} || '00'

Response data field =
T_{PV} || L_{PV} || PV || T_{CC} || L_{CC} || CC

F.6 ENVELOPE command

The use of the ENVELOPE command (see 7.2) is shown.

Command data field =
$T_{PI\ CG}$ || $L_{PI\ CG}$ || PI || CG

Data carried by CG =
Command APDU (starting by CH)
and padding bytes according to PI

Response data field =
$T_{PI\ CG}$ || $L_{PI\ CG}$ || PI || CG

Data carried by CG =
Response APDU
and padding bytes according to PI