
**Financial transaction cards — Messages
between the integrated circuit card and the
card accepting device —**

Part 2:

Functions, messages (commands and
responses), data elements and structures

*Cartes de transactions financières — Messages entre la carte à circuit
intégré et le dispositif d'acceptation des cartes —*

*Partie 2: Fonctions, messages (commandes et réponses), éléments de
données et structures*



Contents

	Page
1 Scope.....	5
2 Normative references.....	5
3 Definitions and abbreviations.....	6
3.1 Definitions.....	6
3.2 Abbreviations	7
4 Application of interindustry ISO/IEC 7816 series	7
4.1 Physical characteristics of the card	7
4.2 Electrical characteristics and transmission protocols	7
4.3 Data structure.....	7
4.3.1 File organisation	8
4.3.2 File referencing.....	8
4.3.3 Elementary file structures.....	8
4.3.4 Data referencing methods.....	8
4.3.5 File control information.....	8
4.4 Security architecture of the card.....	8
4.4.1 Security status.....	8
4.4.2 Security attributes	8
4.4.3 Security mechanisms	8
4.5 Message structure.....	8
4.5.1 Command APDU	8
4.5.2 Response APDU.....	8
4.5.3 Command APDU conventions.....	8
4.5.4 Coding conventions.....	8
4.5.4.1 Class byte	8
4.5.4.2 Instruction byte	8

© ISO 1998

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet central@iso.ch
X.400 c=ch; a=400net; p=iso; o=isocs; s=central

Printed in Switzerland

4.5.4.3 Parameter bytes	8
4.5.4.4 Data field bytes.....	9
4.5.4.5 Status bytes	9
4.6 Logical channels	9
4.7 Secure messaging.....	9
4.8 Basic interindustry commands	9
4.8.1 READ_RECORD(S) command.....	9
4.8.2 APPEND_RECORD command.....	9
4.8.3 UPDATE_RECORD command.....	9
4.8.4 GET_DATA command	10
4.8.5 SELECT_FILE command	10
4.8.6 VERIFY command.....	10
4.8.7 INTERNAL_AUTHENTICATE command.....	10
4.8.8 GET_CHALLENGE command	11
4.8.9 EXTERNAL_AUTHENTICATE command.....	11
4.8.10 GET_RESPONSE command.....	11
4.9 Historical bytes.....	11
5 Application of ISO 10202	12
5.1 Card life cycle.....	12
5.1.1 Manufacture of the IC and ICC.....	12
5.1.2 Card preparation.....	12
5.1.3 ADF preparation.....	12
5.1.4 Card usage.....	12
5.1.5 Termination of use.....	12
5.1.6 Data elements.....	12
5.2 Transaction process	12
5.3 Cryptographic key relationships	12
5.4 Secure Application Modules (SAM).....	12
5.5 Use of algorithms.....	12
5.6 Cardholder verification.....	12
5.7 Key management.....	12
6 Functions	12
6.0 Introduction.....	12
6.1 Card session initialisation.....	13
6.2 CDF/ADF authentication.....	14
6.3 CAD authentication.....	17
6.4 Cardholder verification - decision made by the ICC	18
6.5 ADF selection	19

6.6 Transaction authorisation - decision made by the CAD	20
6.7 Transaction recording.....	21
6.8 Transaction Cryptogram Code (TCC) generation.....	22
6.9 Transaction termination	23
7 Messages (commands and responses).....	23
7.1 DEACTIVATE_FILE.....	23
7.2 GENERATE_TCC.....	24
7.3 GET_PROCESSING_OPTIONS.....	24
8 Data elements and their organisation.....	25
8.1 Data elements.....	25
8.1.1 Card specific data	25
8.1.2 Cardholder and Card Issuer specific data.....	25
8.1.3 Application Supplier specific data.....	27
8.1.4 Authorisation data.....	28
8.1.5 Data elements for logging	30
8.1.6 Authentication data	31
8.2 Table of data elements.....	32
8.2.1 Card specific data	33
8.2.2 Cardholder and Card Issuer specific data.....	33
8.2.4 Authorisation data.....	35
8.2.5 Data elements for logging	36
8.2.6 Authentication data	36
8.2.7 Algorithm and Key identifiers.....	37
8.3 Referencing of data elements.....	37
8.3.1 Management of data elements.....	37
8.3.2 Coding of data as seen at the interface.....	37
8.3.3 Mapping of data elements into constructed templates	37
8.3.4 Tables of constructed templates.....	39
8.3.5 Division of large templates.....	39
8.4 Mapping of constructed templates into Elementary Files.....	39
8.5 Types of ICC logical structures.....	39
Annex A.....	41
Annex B.....	44
Annex C.....	46
Annex D.....	47
Annex E.....	48
E.1 Biometric verification - decision made by the CAD	48
E.2 Transaction authorisation - decision made by the ICC.....	49
Annex F.....	51

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 9992-2 was prepared by Technical Committee ISO/TC 68, *Banking securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

ISO 9992 consists of the following parts, under the general title *Financial transaction cards — Messages between the integrated circuit card and the card accepting device*:

- *Part 1: Concepts and structures*
- *Part 2: Functions, messages (commands and responses), data elements and structures*
- *Part 4: Common data for interchange*

Annex A forms an integral part of this part of ISO 9992. Annexes B to F are for information only.

Financial transaction cards — Messages between the integrated circuit card and the card accepting device —

Part 2:

Functions, messages (commands and responses), data elements and structures

1 Scope

This International Standard is applicable to the use of Integrated Circuit(s) Cards issued by Financial Institutions in retail financial applications in an interchange environment. It specifically addresses :

- the functions required for financial interchange ;
- the messages (commands and responses) between the Integrated Circuit(s) Card (ICC) and the Card Accepting Device (CAD) to effect those functions : generic commands and responses are taken from ISO/IEC 7816-4 and when these are insufficient, this International Standard provides the required commands and responses ;
- the identification and definition of data elements which may or shall be used during exchanges between the ICC and the CAD ;
- the logical structure of files and records used in messages and how data elements are mapped into these messages.

This part of ISO 9992 describes the application of the rules of interindustry Standards ISO/IEC 7816 series, to use IC Cards in international interchange for financial transactions.

This part gives the methods to implement the security architecture described in ISO 10202 series of International Standards to achieve the security requirements for financial transactions.

It initially describes the functions, messages and data elements which may be needed for financial transactions. In the future, additional functions, messages or data elements may be considered to cover the following maintenance operations in international interchange : ADF allocation, personalisation, activation, deactivation, reactivation, termination and key termination, and CDF deactivation and reactivation.

This International Standard is independent of the capabilities of the CAD (connectable or not, attended or unattended) and its status at the time of the transaction (on-line or off-line).

This International Standard is based on the existence of a logical data structure and provides rules for the way data in the ICC are logically referenced by the CAD. It does not define how data are physically structured in the ICC.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this international Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 639:1988, *Code for the representation of names of languages*.

ISO 3166-1:1997, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.

ISO 4217 : 1995, *Codes for the representation of currencies and funds*.

ISO 4909 : 1987, *Bank cards - Magnetic stripe data content for track 3*.

ISO 7810 : 1995, *Identification cards - Physical characteristics*.

ISO 7812:1993, *Identification cards – Identification of issuers*.

ISO 7813 : 1995, *Identification cards - Financial transaction cards*.

ISO/IEC 7816-1 : 1987, *Identification cards - Integrated circuit(s) cards with contacts. Part 1: Physical characteristics*.

ISO/IEC 7816-2 : 1988, *Identification cards - Integrated circuit(s) cards with contacts. Part 2 : Dimension and location of the contacts*.

ISO/IEC 7816-3 : 1989, *Identification cards - Integrated circuit(s) cards with contacts.*
Part 3 : *Electronic signals and transmission protocols*

ISO/IEC 7816-3/Amendment-1:1992, *Identification cards - Integrated circuit(s) cards with contacts.*
Part 3: *Electronic signals and transmission protocols - AMENDMENT 1: Protocol type T = 1, asynchronous half duplex block transmission protocol.*

ISO/IEC 7816-3/Amendment-2:1994, *Identification cards - Integrated circuit(s) cards with contacts.*
Part 3: *Electronic signals and transmission protocols - AMENDMENT 2: Revision of protocol type selection.*

ISO/IEC 7816-4 : 1995, *Identification cards - Integrated circuit(s) cards with contacts.*
Part 4 : *Interindustry commands for interchange.*

ISO/IEC 7816-5 : 1994, *Identification cards - Integrated circuit(s) cards with contacts.*
Part 5 : *Numbering system and registration procedure for application identifiers.*

ISO/IEC 7816-6 : 1996, *Identification cards - Integrated circuit(s) cards with contacts.*
Part 6 : *Interindustry data elements.*

ISO 8583:1993, *Financial transaction card originated messages - Interchange message specifications.*

ISO/IEC 8824:1990, *Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)*

ISO 8859-1:1987, *Information processing - 8-bit single-byte coded graphic character sets -*
Part 1: *Latin alphabet No. 1.*

ISO 8908:1993, *Banking and related financial services - Vocabulary and data elements.*

ISO 9564-1:1991, *Banking - Personal Identification Number management and security - Part 1: PIN protection principles and techniques.*

ISO 9992-1:1990, *Financial transaction cards - Messages between the integrated circuit card and the card accepting device. Part 1: Concepts and structures.*

ISO 10202-1 : 1991, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit(s) cards - Part 1 : Card Life Cycle*

ISO 10202-2 : 1996, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit(s) cards - Part 2 : Transaction Process*

ISO 10202-3 : ----¹⁾, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit(s) cards - Part 3 : Cryptographic Key Relationships*

ISO 10202-4 : 1996, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit(s) cards - Part 4 : Secure Application Modules*

ISO 10202-5 : ----¹⁾, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit(s) cards - Part 5 : Use of Algorithms*

ISO 10202-6 : 1994, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit(s) cards - Part 6 : Cardholder Verification*

ISO 10202-7 : ----¹⁾, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit(s) cards - Part 7 : Key Management*

ISO 10202-8 : ----¹⁾, *Financial transaction cards - Security architectures of financial transaction systems using integrated circuit(s) cards - Part 8 : General principles and overview*

3 Definitions and abbreviations

3.1 Definitions

For the purpose of this International Standard, the following definitions apply.

Application data file (ADF) : A file that supports one or more services.

Card Accepting Device (CAD) : The device used to interface with the Integrated Circuit(s) Card.

Card acceptor : The party accepting the card for the provision of goods or services.

CDF activator : The entity who prepares the ICC for use in financial transactions by the cardholder.

Command : A request or advice message which initiates an action.

Common Data File (CDF) : A file that contains the common data elements stored in the ICC and used to describe the card, the card issuer and the cardholder.

Current file : The most recently selected file.

Data element : Item of information seen at the interface for which is defined a name, a description of logical content, a format and a coding.

Derivation Parameter (DP) : A data element (or a combination of several data elements), contained in an ICC, used to derive key value(s) specific to this ICC, from a seed key. To be suitable for derivation, the (combination of) data element(s) shall be according to ISO 10202-7.

Dedicated File (DF) : A file containing file control information and, optionally, memory available for allocation. It may be the parent of EFs and/or DFs.

Elementary File (EF) : Set of data units or records which share the same file identifier. It cannot be the parent of another file.

File : An organised set of data elements and/or program code in the ICC.

1) To be published

Function : A process accomplished by one or more commands and resultant actions which is used to perform a whole - or part of - a transaction.

Integrated Circuit(s) Card (ICC) : An ID-1 type card (see ISO 7810) into which has been embedded one or more integrated circuits.

Interchange kernel : The minimum set of facilities required to achieve international interchange independently of the card logical structure :

- the complete set of functions required in the CAD to perform an interchange transaction together with the mechanism allowing the selection of options within these functions,
- the set of interindustry commands and responses to perform the required functions,
- the mandatory data elements,
- the mandatory elementary files.

Interchange profile : A mandatory data element describing the capabilities available in the ICC to perform an interchange transaction. This will allow the selection of relevant functions located in the CAD.

Master File (MF) : The mandatory unique dedicated file representing the root of the file structure.

Message : An ordered series of characters transmitted from the CAD to the ICC or vice-versa.

Minor Unit : The precise amount of the transaction, to the smallest denomination of the currency.

Record : A structure as defined in ISO/IEC 7816-4. A record contains one or more data elements.

Response : A message returned to the initiator after the processing of a command by the recipient. It is composed of data (optional) and a mandatory status as described in ISO/IEC 7816-4.

Security status : The result of the composition of procedures related to the identification and/or authentication of the involved entities, if any.

NOTE : See also ISO 8908 for other definitions.

3.2 Abbreviations

The following abbreviations are used in the "*Format*" sections and in the "format" columns of clause 8 :

- a alphabetic character only
- an alpha numeric character only
- ans alpha + numeric + special only
- b binary
- h hexadecimal character
- n numeric character only
- ns numeric with special characters
- s special characters (e.g. decimal mark)

Hexadecimal value XX is noted as h'XX' or as 'xx'.

ATC : Application Transaction Counter

DF : Dedicated File

OAC : On-line Authorisation Code

RAND : Random number

RC : Referral Code

TAC : Transaction Authorisation Code.

TC : Transaction Certificate

TCC : Transaction Cryptogram Code

TDC : Transaction Denial Code

TLV : Tag Length Value

NOTE : (#xxx) refers to data element #xxx as described in clause 8.

4 Application of interindustry ISO/IEC 7816 series

This International Standard is based on ISO/IEC 7816. This clause specifies the application of ISO/IEC 7816 series to perform financial transactions.

4.1 Physical characteristics of the card

An IC card for financial transactions shall be an ID 1 card with Integrated Circuit(s), according to ISO / IEC 7816-1 and 7816-2, with the following qualification :

The contacts shall be located on the front side of the card, as defined in ISO 7810 (same side as the embossing, and the opposite side to the ISO magnetic stripe).

4.2 Electrical characteristics and transmission protocols

The electrical characteristics and transmission protocols of the ICC shall comply with ISO/IEC 7816-3 with the following qualifications :

1. The consumption (I_{CC}) on V_{CC} should never exceed 50 mA.

2. V_{PP} contact is not used.

3. The value of 372 for the clock rate conversion factor and the value of 1 for the bit rate adjustment factor shall be supported (parameters $F = 372$ and $D = 1$).

4. Both protocols $T=0$ and $T=1$ shall be implemented in the CAD to handle ICCs for international interchange. The ICC shall support either $T=0$ or $T=1$ protocol.

5. PTS command is not required.

6. Several historical characters are recommended, see subclause 4.9

4.3 Data structure

This International Standard supports the data structure described in ISO/IEC 7816-4, subclause 5.1.

The industry specific data organisation and referencing within the data structure are defined in clause 8.

4.3.1 File organisation

This International Standard supports the file organisation described in ISO/IEC 7816-4, subclause 5.1.1

4.3.2 File referencing

This International Standard supports the file referencing methods described in ISO/IEC 7816-4, subclause 5.1.2 with the following qualifications :

- referencing by path is not supported,
- referencing by name is conditional,
- referencing by short EF identifier shall be supported.

The First Software Function Table of the Historical Bytes (if present) indicates which referencing methods are supported.

When the historical bytes are not present or do not include the First Software Function Table, the following options are the default values (value h'86' is assumed) :

- DF selection by full name,
- EF management by short EF-ID and record number.

4.3.3 Elementary file structures

This International Standard supports the file organisation described in ISO/IEC 7816-4, subclause 5.1.3 with the following qualification :

The following Elementary File structures defined in ISO/IEC 7816-4 are supported:

linear fixed,
linear variable,
cyclic.

4.3.4 Data referencing methods

This International Standard supports the data referencing methods described in ISO/IEC 7816-4, subclause 5.1.4 with the following qualifications :

1. Referencing by record identifier is not supported.
2. Data unit referencing is not supported.

4.3.5 File control information

This International Standard supports the File Control Information described in ISO/IEC 7816-4, subclause 5.1.5 at DF level only.

4.4 Security architecture of the card

This International Standard supports the Security Architecture of the Card described in ISO/IEC 7816-4, subclause 5.2.

4.4.1 Security status

This International Standard supports the security status described in ISO/IEC 7816-4, subclause 5.2.1.

The value of SW1-SW2 may be used by the ICC to request an on-line EXTERNAL AUTHENTICATE command.

SW1 = h'92'.

SW2 = to be defined by the Application Supplier.

4.4.2 Security attributes

This International Standard supports the security attributes described in ISO/IEC 7816-4, subclause 5.2.2.

4.4.3 Security mechanisms

This International Standard supports the security mechanisms described in ISO/IEC 7816-4, subclause 5.2.3.

4.5 Message structure

4.5.1 Command APDU

This International Standard supports the Command APDU structure described in ISO/IEC 7816-4, subclause 5.3.1.

The highest L_c accepted is 256 bytes.

4.5.2 Response APDU

This International Standard supports the Response APDU described in ISO/IEC 7816-4, subclause 5.3.3.

4.5.3 Command APDU conventions

This International Standard supports the command APDU conventions described in ISO/IEC 7816-4, subclause 5.4.

4.5.4 Coding conventions

4.5.4.1 Class byte

This International Standard supports the coding conventions described in ISO/IEC 7816-4, subclause 5.4.1 with the following qualifications :

1. The commands described in ISO/IEC 7816-4, supported by this International Standard, shall be coded with the most significant nibble = h'0'.

2. The industry specific commands described in this International Standard shall be coded with the most significant nibble = h'B', and the least significant nibble shall be coded in accordance with the convention described in ISO/IEC 7816-4, table 9.

4.5.4.2 Instruction byte

This International Standard supports the coding conventions described in ISO/IEC 7816-4, subclause 5.4.2. Additional industry specific codes are defined in clause 7.

4.5.4.3 Parameter bytes

This International Standard supports the coding conventions described in ISO/IEC 7816-4, subclause 5.4.3. Additional industry specific codes are defined in clause 7.

4.5.4.4 Data field bytes

This International Standard supports the coding conventions described in ISO/IEC 7816-4, subclause 5.4.4.

4.5.4.5 Status bytes

This International Standard supports the coding conventions described in ISO/IEC 7816-4, subclause 5.4.5 with the following qualifications :

1. For the interindustry commands, all status bytes described in ISO/IEC 7816-4 are applicable.

2. For industry specific commands, two additional application dependant SW1 status bytes are defined as following :

SW1 = h'9E' for warning processing with further industry specific qualification in SW2.

SW1 = h'9F' for execution error with further industry specific qualification in SW2.

4.6 Logical channels

This International Standard supports the logical channels described in ISO/IEC 7816-4, subclause 5.5 with the following qualifications :

When a financial transaction card supports the logical channel mechanisms,

1. this option shall be described in the Third Software Function Table of the ATR file or Historical Bytes.

2. the logical channel 0 (default) shall always be available to perform international interchange transactions.

4.7 Secure messaging

This International Standard does not mandate use of secure messaging as described in ISO/IEC 7816-4 for financial transactions. When used, secure messaging shall be implemented as described in ISO/IEC 7816-4.

4.8 Basic interindustry commands

The following basic interindustry commands defined in ISO/IEC 7816-4 which are issued by the CAD are supported by this International Standard :

1. READ_RECORD(S)
2. APPEND_RECORD
3. UPDATE_RECORD
4. GET_DATA
5. SELECT_FILE
6. VERIFY
7. INTERNAL_AUTHENTICATE
8. EXTERNAL_AUTHENTICATE
9. GET_CHALLENGE
10. GET_RESPONSE

Implementation of READ_RECORD(S) command is mandatory in the ICC and in the CAD. All other commands are optional.

The following subclauses describe for each command the options supported by this International Standard.

4.8.1 READ_RECORD(S) command

4.8.1.1 Definition and scope

According to ISO/IEC 7816-4 subclause 6.5.1.

This command should be used to read one record of an EF of linear or cyclic structure.

4.8.1.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.5.2.

4.8.1.3 Command message

According to ISO/IEC 7816-4 subclause 6.5.3, with the following qualification :

The last significant three bits in P2 shall be b'100'.

4.8.1.4 Response message

According to ISO/IEC 7816-4 subclause 6.5.4 with the following qualification:

The coding of the data field of the response shall be the case b (complete read of one record).

4.8.1.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.5.5.

4.8.2 APPEND_RECORD command

4.8.2.1 Definition and scope

According to ISO/IEC 7816-4 subclause 6.7.1

This command should be used to append a record in an EF of linear or cyclic structure.

When this command is supported, the two least significant bits of the First Software Function Table of the card capabilities of the Historical Bytes, as defined in ISO/IEC 7816-4 subclause 8.3.6, shall be set to b'10'.

4.8.2.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.7.2.

4.8.2.3 Command message

According to ISO/IEC 7816-4 subclause 6.7.3.

4.8.2.4 Response message

According to ISO/IEC 7816-4 subclause 6.7.4.

4.8.2.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.7.5.

4.8.3 UPDATE_RECORD command

4.8.3.1 Definition and scope

According to ISO/IEC 7816-4 subclause 6.8.1

This command should be used to update a record in an EF of linear structure.

4.8.3.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.8.2.

4.8.3.3 Command message

According to ISO/IEC 7816-4 subclause 6.8.3.

4.8.3.4 Response message

According to ISO/IEC 7816-4 subclause 6.8.4.

4.8.3.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.8.5.

4.8.4 GET_DATA command

4.8.4.1 Definition and scope

According to ISO/IEC 7816-4 subclause 6.9.1

An example of this command is to retrieve a primitive data object dynamically managed by the ICC, such as a PIN try counter or a transaction counter.

Depending on the implementation chosen by the issuer, the data element retrieved by this command may be shared with other applications or only managed by the active application, i.e. the one that was previously selected.

4.8.4.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.9.2.

4.8.4.3 Command message

According to ISO/IEC 7816-4 subclause 6.9.3.

4.8.4.4 Response message

According to ISO/IEC 7816-4 subclause 6.9.4.

4.8.4.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.9.5.

4.8.5 SELECT_FILE command

4.8.5.1 Definition and scope

According to ISO/IEC 7816-4, subclause 6.11.1, with the following qualification :

This International Standard supports the following Dedicated File selections:

- DF name (P1 = h'04')
- file-identifier as a child DF (P1 = h'01')
- parent DF (P1 = h'03')

4.8.5.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.11.2.

4.8.5.3 Command message

According to ISO/IEC 7816-4 subclause 6.11.3.

4.8.5.4 Response message

According to ISO/IEC 7816-4 subclause 6.11.4.

4.8.5.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.11.5.

4.8.6 VERIFY command

4.8.6.1 Definition and scope

According to ISO/IEC 7816-4 subclause 6.12.1.

4.8.6.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.12.2 with the following qualifications :

- 1 The number of consecutive unsuccessful comparisons shall be counted and recorded in the card.

- 2 The number of unsuccessful retries in the error counter should be reset following a successful comparison.

4.8.6.3 Command message

According to ISO/IEC 7816-4 subclause 6.12.3.

4.8.6.4 Response message

According to ISO/IEC 7816-4 subclause 6.12.4.

4.8.6.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.12.5 with the following qualification :

When the verification is completed but unsuccessful, SW1 = h'63' and SW2 should indicate the number of retries left, and the coding is according to subclause 5.4.5 of ISO/IEC 7816-4.

4.8.7 INTERNAL_AUTHENTICATE command

4.8.7.1 Definition and scope

According to ISO/IEC 7816-4 subclause 6.13.1.

4.8.7.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.13.2.

4.8.7.3 Command message

According to ISO/IEC 7816-4 subclause 6.13.3 with the following qualifications :

P1 shall be coded h'00'.

The data field contains data element #604 and optionally data elements #601 and #107.

4.8.7.4 Response message

According to ISO/IEC 7816-4 subclause 6.13.4 with the following qualification :

The authentication related data is data element #605.

4.8.7.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.13.5.

4.8.8 GET_CHALLENGE command

4.8.8.1 Definition and scope

According to ISO/IEC 7816-4 subclause 6.15.1.

4.8.8.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.15.2.

4.8.8.3 Command message

According to ISO/IEC 7816-4 subclause 6.15.3.

4.8.8.4 Response message

According to ISO/IEC 7816-4 subclause 6.15.4 with the following qualification :

The data field shall consist of the ICC challenge (data element #606).

4.8.8.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.15.5.

4.8.9 EXTERNAL_AUTHENTICATE command

4.8.9.1 Definition and scope

According to ISO/IEC 7816-4 subclause 6.14.1.

4.8.9.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 6.14.2.

4.8.9.3 Command message

According to ISO/IEC 7816-4 subclause 6.14.3 with the following qualifications :

P1 shall be coded h'00'.

The authentication related data are data elements #607, #107 and #601.

4.8.9.4 Response message

According to ISO/IEC 7816-4 subclause 6.14.4.

4.8.9.5 Status conditions

According to ISO/IEC 7816-4 subclause 6.14.5.

4.8.10 GET_RESPONSE command

4.8.10.1 Definition and scope

According to ISO/IEC 7816-4 subclause 7.1.1 with the following qualification :

The purpose is to supply the CAD with data resulting from a previous action undertaken by the ICC and temporarily stored in its memory.

4.8.10.2 Conditional usage and security

According to ISO/IEC 7816-4 subclause 7.1.2.

4.8.10.3 Command message

According to ISO/IEC 7816-4 subclause 7.1.3.

4.8.10.4 Response message

According to ISO/IEC 7816-4 subclause 7.1.4.

4.8.10.5 Status conditions

According to ISO/IEC 7816-4 subclause 7.1.5.

4.9 Historical bytes

The Historical Bytes, defined in subclause 8.3 of ISO/IEC 7816-4, provide an ability for the CAD to receive early knowledge of some characteristics of the IC. The presence of the historical bytes is optional. The information carried by the historical bytes may also be found in an ATR file.

If the historical bytes are absent, the default characteristics of the IC are as follows :

- file I/O services by READ_RECORD command,
- DF selection by full DF name,
- write OR,
- data unit size is one byte,
- short L_C and L_E fields,
- logical channel 0 only supported.

If the historical bytes are present, and the card service data, the pre-issuing data and the card capabilities data are not specified, then the default values for these elements are the ones defined in subclauses 4.9.1 and 4.9.3.

4.9.1 Card service data

The card service data, described in subclause 8.3.2 of ISO/IEC 7816-4, has the tag and length h'31'.

The default value is h'80'. This value provides :

- direct application selection by full DF name,
- data objects not available in DIR file,
- data objects not available in ATR file,
- file I/O services by READ_RECORD(S) command.

4.9.2 Pre-issuing data

This data object (tag and length h'6Y') does not have a specific format or content according to subclause 8.3.5 of ISO/IEC 7816-4. For this International Standard, the data object has the tag and length h'67' and contains the following data elements in the order specified :

- IC manufacturer identifier (#101) (one byte),
- Manufacturer's IC type identifier (#102) (two bytes),
- IC serial number (#105) (4 bytes).

4.9.3 Card capabilities

This data object, described in subclause 8.3.6 of ISO/IEC 7816-4, may have one of three tags. It may contain either the First Software Function Table (tag h'71'), the First two Software Function Tables (tag h'72') or the three Software Function Tables (tag h'73').

The default values are :

- First Software Function Table : h'86',
- Second Software Function Table : h'41',
- Third Software Function Table : h'00'.

These values provide :

- DF selection by full DF name,
- EF management : short EF identifier supported and record number supported,
- behaviour of write function : write OR,
- data unit size : one byte,
- short L_C and L_E fields,
- one logical channel.

5 Application of ISO 10202

This clause is divided into subclauses that correspond to each part of 10202.

5.1 Card life cycle

5.1.1 Manufacture of the IC and ICC

This part of this International Standard does not specify messages to be used for this step of the card life cycle.

5.1.2 Card preparation

This part of this International Standard does not specify messages to be used for this step of the card life cycle.

5.1.3 ADF preparation

This part of this International Standard does not specify messages and data elements to be used for this step of the card life cycle.

5.1.4 Card usage

Clause 6 of this International Standard defines the functions related to card usage.

5.1.5 Termination of use

This part of this International Standard does not specify messages and data elements to be used for this step of the card life cycle.

5.1.6 Data elements

5.1.6.1 IC manufacturer ID

(#101), defined in subclause 8.1.1.1.

5.1.6.2 Manufacturer's IC type identifier

(#102), defined in subclause 8.1.1.2.

5.1.6.3 Embedder/IC assembler Identifier

(#103), defined in subclause 8.1.1.3.

5.1.6.4 Card personaliser Identifier

(#201), defined in subclause 8.1.2.1.

5.1.6.5 CDF activator identifier

(#206), defined in subclause 8.1.2.6.

5.1.6.6 CDF activator serial number

(#207), defined in subclause 8.1.2.7.

5.1.6.7 Card effective date

(#208), defined in subclause 8.1.2.8.

5.2 Transaction process

Clause 6 of this part of this International Standard specifies the functions to achieve the Transaction Process according to the security functions defined in ISO 10202-2.

5.3 Cryptographic key relationships

The subset of Issuer and Application Supplier keys, defined in ISO 10202-3, which is used in Transaction Process, is described in subclause 8.2.7 of this International Standard.

The other keys, related to other steps of the Card Life Cycle, defined in ISO 10202-3, are not described in this part of this International Standard.

5.4 Secure Application Modules (SAM)

Messages and data elements to be used between CAD and SAM are not defined in this part of this International Standard.

5.5 Use of algorithms

ISO 10202-5 describes a range of algorithms that can be used to deliver a variety of security services (e.g. entity authentication). This International Standard makes use of similar security services as considered in clause 6.

5.6 Cardholder verification

Subclause 4.2 of ISO 10202-6 is covered by subclause 6.4.2 of this part of this International Standard.

5.7 Key management

Key management is outside the scope of this International Standard.

6 Functions

6.0 Introduction

This clause identifies and defines the structure and use of each function that may be used to support financial

interchange. The definition of each function is provided in four parts. The *Name* (6.x) identifies the specific function; the *Purpose* (6.x.1) defines the objective(s); the *Description* (6.x.2) provides a narrative defining how the function is performed; and the *Process flow* (6.x.3) describes a series of actions and the use of messages (commands and responses) including data elements required to complete the function. The process flow is followed by a table that illustrates the sequence of actions, decisions and messages.

The only mandatory function is Card Session Initialisation, which follows the Answer to Reset. All the other functions in this document are not mandatory, but if implemented the sequence of messages shall be as described in the relevant tables.

Actions and resultant decisions shown in the tables are for information only.

All functions are initiated by the CAD, although this is not meant to imply that the decision-making is performed in the CAD, which is determined by the technology and the specific implementation deployed.

The description of actions and decisions made by the CAD does not imply that they shall be performed in an off-line environment. The CAD may be connected on-line to a device (e.g. SAM, Host) that performs the specific actions and decisions described in the standard. However, whether the action or decision is completed in the CAD or by another device does not affect the function and its related messages, commands and responses, as defined as the interaction between the CAD and the ICC, but it may affect the sequence of functions and messages.

When the name of a command appears in capital letters (e.g. READ), it should be understood as the generic name for the command. It encompasses one or more occurrences of the same message using this command as defined in subclause 4.8 or clause 7 of this part of this International standard.

The following functions are supported by this International Standard :

1. CARD SESSION INITIALISATION
2. CDF/ADF AUTHENTICATION
3. CAD AUTHENTICATION

4. CARDHOLDER VERIFICATION
5. ADF SELECTION
6. TRANSACTION AUTHORISATION-DECISION MADE BY THE CAD
7. TRANSACTION RECORDING
8. TRANSACTION CRYPTOGRAM CODE (TCC) GENERATION
9. TRANSACTION TERMINATION

It is assumed that all cryptographic functions that involve a secret key of a symmetric algorithm or an asymmetric algorithm are performed in a SAM or a CAD that is a physically secure device (ISO 10202-4 and ISO 10202-7). Cryptographic functions performed using a public key of a cryptographic algorithm may be performed in a CAD that is not a physically secure device provided that the requirements of ISO 10202-7 are met.

6.1 Card session initialisation

6.1.1 Purpose

To ensure that the CAD and the ICC are physically and logically compatible, and that the ICC is intended for financial transactions in accordance with this International Standard. This function is mandatory at the beginning of each session.

6.1.2 Description

A check shall be carried out to ensure that the CAD and the ICC are physically and logically compatible and that the ICC may be used for financial transactions after its capabilities are determined.

6.1.3 Process flow (see table 1)

The CAD analyses the ICC physical characteristics and the parameters resulting from the answer to reset. Where these parameters and characteristics do not match CAD capabilities, and default values, as defined in ISO/IEC 7816-3, cannot be used, the session shall be aborted.

In order to determine whether the ICC may be used for

CAD A1 A2		ICC
Reference	Description	Parameters and data
A1	Analyse answer to reset	
A2	Check with card logical structure indicator how the transaction can be conducted	

Table 1 - Card session initialisation

financial transactions, data may be retrieved from one of more files (such as the COP_EF) or by some other techniques (such as application selection by identifier).

The status of the ICC, as returned in the Historical Bytes (if present) in the answer to reset, shall be checked, to ensure that the session can proceed.

The "card logical structure indicator" is used to determine how to conduct the transaction, and is deduced from the value of the first nibble of the First Software Function Table. It shall be determined from the Historical Bytes or the ATR file (if present) or the default value as defined in subclause 4.9 shall be used.

6.2 CDF/ADF authentication

NOTE : The present subclause is intended for either CDF authentication or ADF authentication. So, in the text, CDF/ADF means either CDF or ADF.

6.2.1 Purpose

To verify that the CDF/ADF has been issued by an entitled authority.

A method using an asymmetric algorithm authenticating the data is addressed under 6.2.2.

A method using a symmetric algorithm in a dynamic fashion is addressed under 6.2.3.

6.2.2 CDF/ADF data authentication using an asymmetric algorithm.

The following process complies with the principles defined in ISO 10202.

6.2.2.1 Description

The CDF/ADF data authentication may be performed either with a one-step procedure or with a two-step procedure. They both use an asymmetric algorithm. An CDF/ADF may offer both possibilities.

The one-step procedure shall be performed in interchange, whenever the parameters of the asymmetric algorithm and the related public key of the key issuer (which may be the card issuer or an application supplier, or their agents) are known to the CAD.

The two-step procedure shall be performed whenever the one-step procedure is not available and whenever the parameters of the asymmetric algorithm and the related public key of the trusted third party are known to the CAD.

6.2.2.2 Process flow for the one-step procedure (see table 2a)

6.2.2.2.1 Determination of the operands to the verification

- 6.2.2.2.1.1 Prior to the transaction, the CAD stores the following information :
- key identifier, which includes :
 - key issuer identifier (part of AID, e.g. IIN or RID),
 - key number,
 - corresponding public key exponent,
 - corresponding public key modulus,
 - date of end of validity of the key, if any.
- 6.2.2.2.1.2 To carry out the authentication of the data, the CAD needs the following information from the CDF/ADF :
- key issuer identifier (AID or IIN or RID),
 - one-step/key number (data element #608),
 - one-step/signed data (data element #609) ;

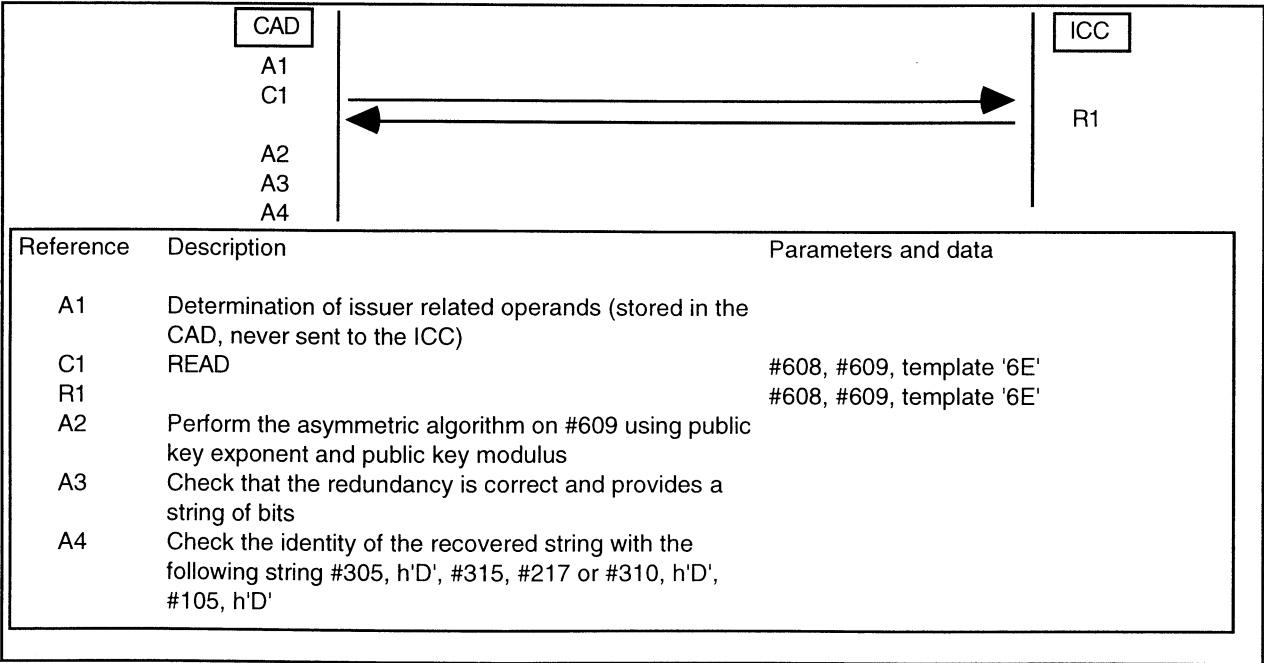


Table 2a -CDF/ADF data authentication using an asymmetric algorithm (one step procedure)

- Cardholder identification number (#305), service code (#315), expiry date (#217 or #310).
- IC serial number (#105).

6.2.2.2.2 One-step authentication process

a) The CAD identifies from the key number (data element #608) obtained from the card, the following data elements stored in the CAD :

- corresponding public key exponent,
- corresponding public key modulus,
- date of the end of validity of the key, if any.

b) The CAD shall verify that the key is valid by comparing the current date and the date of the end of validity of the key, if any.

c) The CAD shall perform the asymmetric algorithm on the one-step/signed data (data element #609) using :

- the asymmetric algorithm,
- the public key exponent,
- the public key modulus.

d) The result is a string of bits which is divided into two parts of identical lengths :

- if the number of bits is odd, the CAD shall verify that the most significant bit is zero. The most significant bit shall be discarded and excluded from the comparison. The CAD shall then verify that the utmost right string of bits and the utmost left string of bits are identical.

e) The CAD shall verify that the identical parts of the bit string (see subclause d) above) are the concatenation of the following successive data elements with delimiters, as obtained from the card (see 6.2.2.2.1.2) :

- Cardholder identification number (#305),
- delimiter h'D',
- service code (#315),
- expiry date (#217 or #310),
- delimiter h'D',
- IC serial number (#105),
- delimiter h'D',
- padded to the right with binary zeros, where necessary.

f) The CAD shall verify that the IC serial number, obtained from the operation e, is identical to the IC serial number read from the card (see subclause 6.2.2.2.1.2).

g) If the procedure is successful, the authentication is performed.

6.2.2.3 Process flow for the two-step procedure (see table 2b)

6.2.2.3.1 Determination of the operands to the verification

6.2.2.3.1.1 Prior to the transaction, the CAD stores the following information :

- trusted third party key identifier, which includes :
 - trusted third party identifier (AID or IIN or RID),
 - two-step/trusted third party key number, data element #610,
 - corresponding public key exponent,
 - corresponding public key modulus,
- date of end of validity of the key, if any.

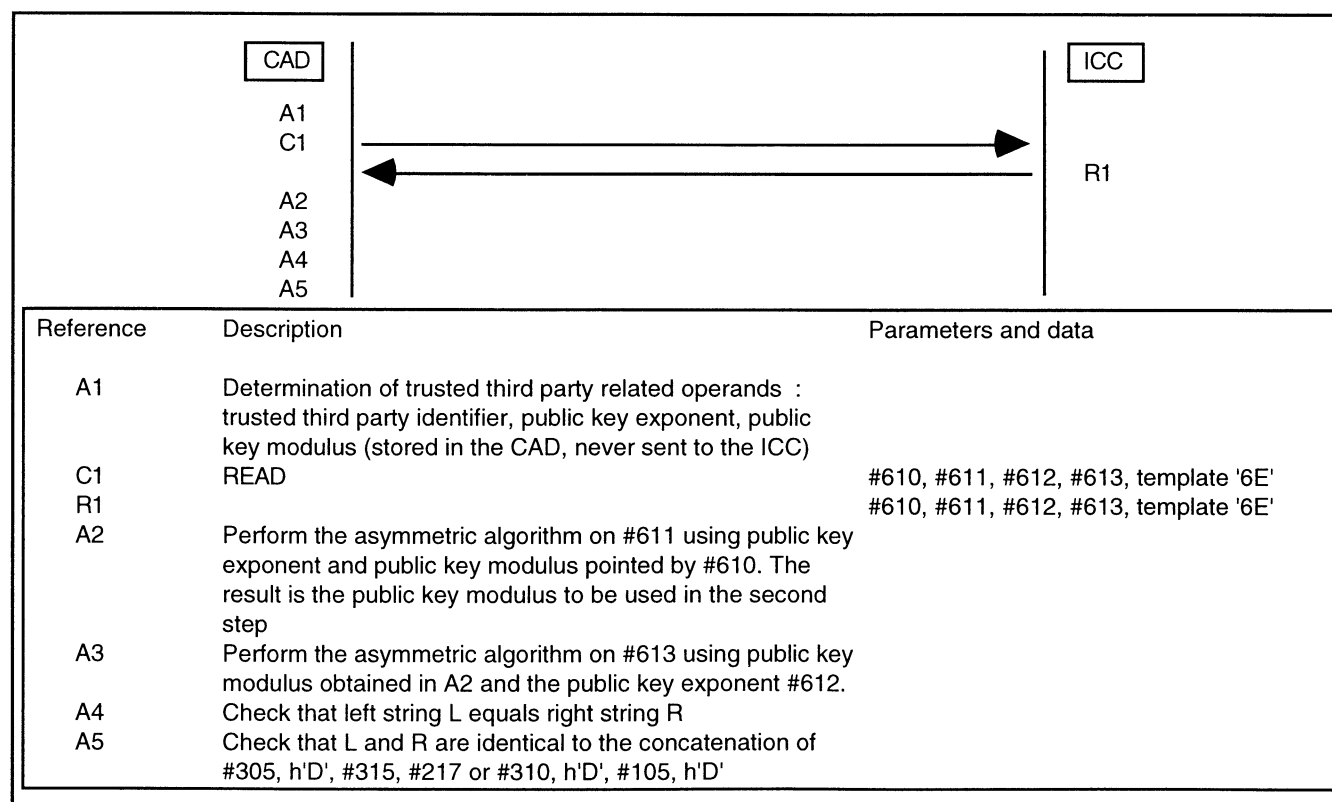


Table 2b -CDF/ADF data authentication using an asymmetric algorithm (two step procedure)