INTERNATIONAL STANDARD

ISO 9992-2

First edition
1998-04-15

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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 (commands et réponses), éléments de données et structures

Reference number
ISO 9992-2:1998(E)

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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

This page intentionally left blank

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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**

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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_e 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.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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 :

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

- 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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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		ICC
A1		
A2		
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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

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)

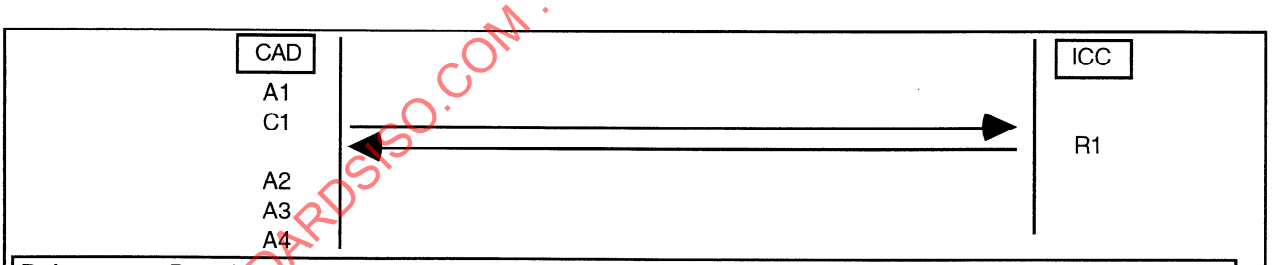
6.2.2.2.1 Determination of the operands to the verification

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) ;



Reference	Description	Parameters and data
A1	Determination of issuer related operands (stored in the CAD, never sent to the ICC)	
C1	READ	#608, #609, template '6E'
R1		#608, #609, template '6E'
A2	Perform the asymmetric algorithm on #609 using public key exponent and public key modulus	
A3	Check that the redundancy is correct and provides a string of bits	
A4	Check the identity of the recovered string with the following string #305, h'D', #315, #217 or #310, h'D', #105, h'D'	

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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

- 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).

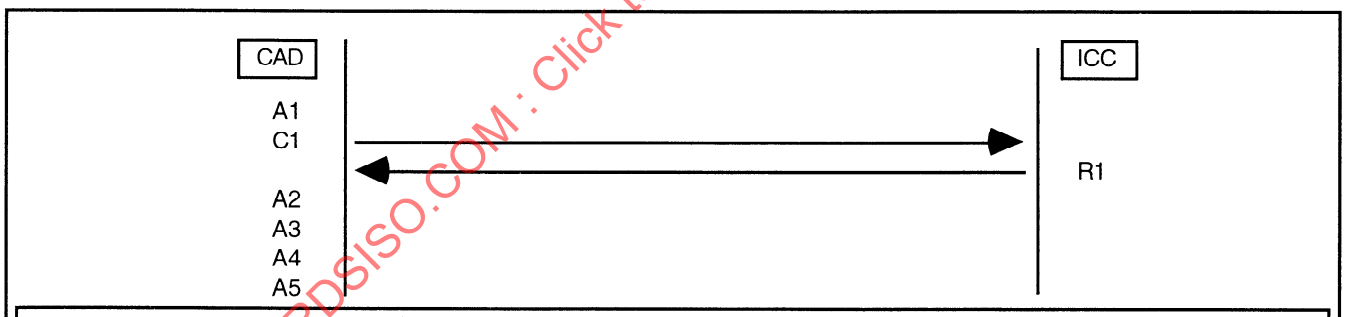
g) If the procedure is successful, the authentication is performed.

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.



Reference	Description	Parameters and data
A1	Determination of trusted third party related operands : trusted third party identifier, public key exponent, public key modulus (stored in the CAD, never sent to the ICC)	
C1	READ	#610, #611, #612, #613, template '6E'
R1		#610, #611, #612, #613, template '6E'
A2	Perform the asymmetric algorithm on #611 using public key exponent and public key modulus pointed by #610. The result is the public key modulus to be used in the second step	
A3	Perform the asymmetric algorithm on #613 using public key modulus obtained in A2 and the public key exponent #612.	
A4	Check that left string L equals right string R	
A5	Check that L and R are identical to the concatenation of #305, h'D', #315, #217 or #310, h'D', #105, h'D'	

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

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

6.2.2.3.1.2 To carry out the authentication of the data, the CAD needs the following information from the CDF/ADF :

- trusted third party identifier (AID or IIN or RID),
- two-step/trusted third party key number, data element (#610),
- two-step/signed data #1, data element (#611),
- two-step/public exponent #2, data element (#612),
- two-step/signed data #2, data element (#613) ,
- Cardholder identification number (#305), service code (#315), expiry date (#217 or #310),
- IC serial number (#105);

6.2.2.3.2 Two-step authentication process

a) The CAD identifies from the trusted third party identifier and the two-step/trusted third party key number (data element #610) obtained from the card (see subclause 6.2.2.3.1.2) the following data elements stored in the CAD (see subclause 6.2.2.3.1.1) :

- corresponding public key exponent,
- corresponding public key modulus,
- date of 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 performs the asymmetric algorithm on the two-step/signed data #1 (data element #611) using :

- the asymmetric algorithm,
- public key exponent of the trusted third party (see subclause 6.2.2.3.2 a),
- the public key modulus of the trusted third party(see subclause 6.2.2.3.2 a).

d) The result is a string of bits which is divided into three fields :

- the 16 first bits represent the length NZ (in BCD) of the binary zeros field which follows,
- a second field, filled with binary zeros,
- the third field represents the public key to be used in the second step. The public key field begins with the first binary 1 after the second field (zeros filled field).

e) The CAD shall verify that :

- NZ is equal or higher than h'0112',
- the second field is filled only with binary zeros,
- the length of the second field is NZ.

f) The CAD identifies from the data element (#612) the exponent associated with the second step procedure.

The CAD shall verify that the exponent is higher or equal to 3. When this data element is not present, the exponent is equal to 3.

g) The CAD performs the asymmetric algorithm of the two-step/signed data #2 (data element #613) using :

- the asymmetric algorithm,
- the public key exponent defined in subclause f) above,
- the public key modulus defined in subclause d) above, third field.

h) The result is a string of bits which is divided into two parts of identical length :

- 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 verify that the utmost right string of bits and the utmost left string of bits are identical.

i) The CAD shall verify that the identical parts of the bit string (see subclause h) above) are the concatenation of the following successive data elements, with delimiters as obtained from the card (see subclause 6.2.2.3.1.2) :

- 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.

j) 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 6.2.2.3.1.2).

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

6.2.3 Dynamic authentication using a symmetric algorithm

6.2.3.1 Description

The method used shall comply with ISO 10202-2 using the selected key described in ISO 10202-3. The proof of the authenticity of the CDF/ADF shall be obtained by verifying that the response to a challenge (e.g. a random number) has been correctly calculated by the CDF/ADF using the selected symmetric authentication algorithm and Key-ID.

The equality of the two results proves the genuineness of the CDF/ADF.

6.2.3.2 Process flow (see table 2c)

KI'aut (key-id is #107) is the derived authentication key provided by the Card Issuer/Application Supplier.

F_A (FA-id is #601) is the cryptographic function (algorithm) used for authentication.

DP (#602) stands for the Derivation Parameter(s) used for the derivation of the authentication key.

F_D (FD-id is #603) is the Derivation Function.

6.2.3.2.1 Determination of authentication parameters

To carry out the authentication of the CDF/ADF, the CAD needs the following information :

- reference to the cryptographic function(s)

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

available in the CDF/ADF,
- reference to the authentication key(s) available in the CDF/ADF,
- derivation parameter(s) and algorithm used for key derivation.

Those parameters which are not known by the CAD shall be obtained by a READ issued by the CAD. If several key-algorithm pairs are supported by the CDF/ADF, the CAD shall eliminate those which do not match its own capabilities. If several possibilities remain, application specific criteria shall be applied for choosing one.

6.2.3.2.2 Random generation and encipherment

The CAD generates a CAD challenge (#604) and requests the CDF/ADF to encipher it via the algorithm and key specified in the command message.

Upon completion of the INTERNAL_AUTHENTICATE command, the CDF/ADF returns the number and a status. A status reflecting an error condition shall lead to an immediate abortion of the function.

6.2.3.2.3 Key reconstruction and encipherment by the CAD

The CAD shall reconstruct the value of the authentication key the CDF/ADF is supposed to contain by deriving it from the card issuer's master key, using the appropriate derivation function F_D and the parameter(s) DP.

It then performs the same encipherment process as the CDF/ADF.

6.2.3.2.4 Decision and final processing

The CAD compares the result of the encipherment it carried out with the one returned by the ICC.

If both results are equal, the CDF/ADF is considered as authentic and the function is successfully terminated.

If the results are not equal, the CDF/ADF shall be considered as non-authentic and the CAD terminates the transaction.

6.3 CAD authentication

6.3.1 Purpose

The CAD-authentication conditionally sets the availability of functions in the CDF/ADF using the result (yes/no) of the computation by the CDF/ADF based on an ICC challenge (#606) issued by the CDF/ADF. This function shall be activated on request of the CDF/ADF by a specific value of SW1-SW2, as specified in ISO/IEC 7816-4 in response to any command.

NOTE : "CAD" covers the interface and includes the authorised end points such as SAM, Host.

6.3.2 Description

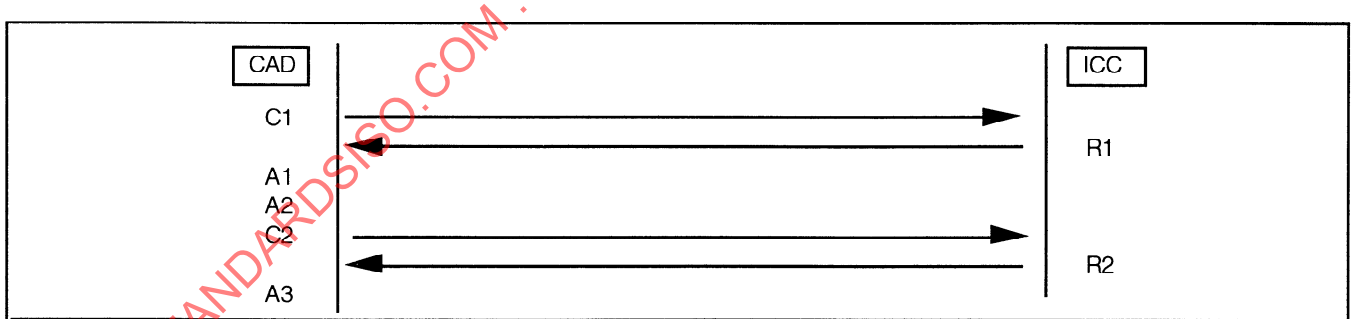
The method used shall comply to ISO 10202-2 using the selected key described in ISO 10202-3. The proof of the authenticity of the CAD shall be obtained by having the CDF/ADF verify the CAD response to a challenge (e.g. a random number) using the selected authentication algorithm and Key ID.

The CDF/ADF, using its own key value, enciphers the challenge. If the result is equal to the result obtained from the CAD, the CDF/ADF considers the CAD legitimate and the card session can proceed.

6.3.3 Process flow (see table 3)

KI'aut is the derived authentication key provided by the Card Issuer.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998



Reference	Description	Parameters and data
C1	READ	#107, #601, #602, #603
R1		#107, #601, #602, #603
A1	Determine key and FA to be used	
A2	Generate random number RAND	
C2	INTERNAL_AUTHENTICATE	#107, #601, #604
R2		ER = FA(KI'aut, RAND), status
A3	Reconstruct key value KI'aut = FD (Klaut,DP) Compute ER Compare	

Table 2c - Dynamic authentication using a symmetric algorithm

F_A is the cryptographic function (algorithm) used for authentication by the CDF/ADF.
DP stands for the Derivation Parameter(s) used for the derivation of the authentication key.
F_D is the Derivation Function.

6.3.3.1 Determination of the authentication parameters

To have itself authenticated by the CDF/ADF, the CAD needs the following information :

- reference to the cryptographic function(s) available in the CDF/ADF,
- reference to the authentication key(s) available in the CDF/ADF,
- derivation parameter(s) and algorithm used for key derivation.

6.3.3.2 Acquisition of challenge

Using the command GET_CHALLENGE, the CAD requests generation of a challenge by the CDF/ADF which shall be returned by the CDF/ADF upon completion of the command. A status reflecting an error condition shall abort the function.

6.3.3.3 Key reconstruction and encipherment by CAD

The CAD shall reconstruct the key value KI'aut the CDF/ADF is supposed to contain by using the derivation parameter(s) DP and the derivation function F_D determined in the first step.

The CAD shall then encipher the challenge provided by the CDF/ADF, using the reconstructed key value KI'aut and the cryptographic function F_A.

6.3.3.4 Authentication by CDF/ADF

The CAD sends an EXTERNAL_AUTHENTICATE to the CDF/ADF, together with the enciphered value of the challenge and the identifiers of the key and algorithm used.

The verification of the authenticity of the CAD is performed for instance as follows : the CDF/ADF enciphers the previously generated challenge and compares the obtained result with the one sent by the CAD.

The CDF/ADF returns a status to the CAD indicating the result of the comparison.

6.3.3.5 Final processing

If the status indicates that the results were equal, the CAD continues with the next function. If the CAD authentication is unsuccessful, the security status of the CDF/ADF shall prevent the execution of any further command which could lead to the successful completion of the transaction.

6.4 Cardholder verification - decision made by the ICC

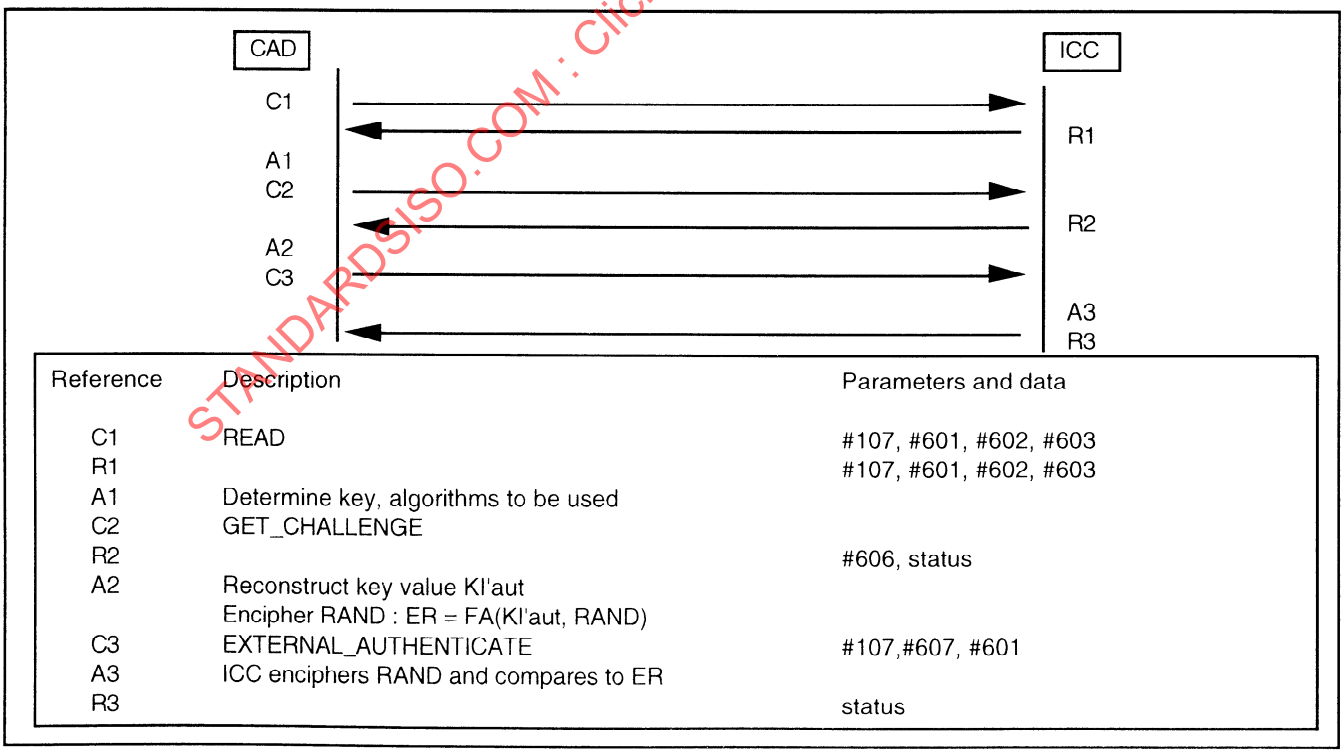
6.4.1 Purpose

To determine that the card presenter is the cardholder.

A method based on ICC decision (e.g. PIN verification) is addressed under 6.4.2.

A method based on CAD decision (e.g. biometric verification, when the ICC is not able to perform the verification) is addressed under E.1 in annex E.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998



Reference	Description	Parameters and data
C1	READ	#107, #601, #602, #603
R1		#107, #601, #602, #603
A1	Determine key, algorithms to be used	
C2	GET_CHALLENGE	
R2		#606, status
A2	Reconstruct key value KI'aut Encipher RAND : ER = FA(KI'aut, RAND)	
C3	EXTERNAL_AUTHENTICATE	#107,#607, #601
A3	ICC enciphers RAND and compares to ER	
R3		status

Table 3 - CAD authentication

The choice of the method is made by the CAD, based on the capabilities of the ICC.

6.4.2 Description

The method used shall comply with ISO 10202-2 and 3. The CAD reads the cardholder identification methods from the ICC and selects one of them.

The CAD acquires data from the presenter of the card.

Data are sent to the ICC.

The ICC according to the method chosen, matches the submitted data against the reference data (stored in the ICC).

The remaining number of attempts shall be recorded in the ICC and should be available to the CAD.

6.4.3 Process flow (see table 4)

6.4.3.1 Negotiation of verification methods

The verification method that applies to the transaction is selected from those available.

6.4.3.2 Acquisition of verification data

This task is accomplished by the CAD and requires no communication with the ICC.

6.4.3.3 Verification by the ICC

The CAD sends the verification data, in plain text, to the ICC for validation.

The ICC checks the verification data against the reference data, records the result and responds with a status code indicating whether the validation was positive or negative and if additional verification attempts are permitted.

6.4.3.4 Decision and final processing

On the basis of the results of the cardholder's verification, a decision is made by the CAD whether to proceed with the transaction.

6.5 ADF selection

6.5.1 Purpose

To establish a logical connection between the CAD and the ADF to be used in international interchange, to check that the ADF is acceptable to the CAD, and optionnally to obtain information on the location of the data to be used.

6.5.2 Description

The selection may be performed using the DF name. After completion of the selection all subsequent commands will have the path to that ADF maintained until another DF is selected. Accessing the data is possible using a GET_PROCESSING_OPTIONS command.

6.5.3 Process flow (see table 5)

6.5.3.1 Determination of selection parameters of available ADFs

The CAD determines the parameters : Application ID (# 321) and optionally the Application label (#304).

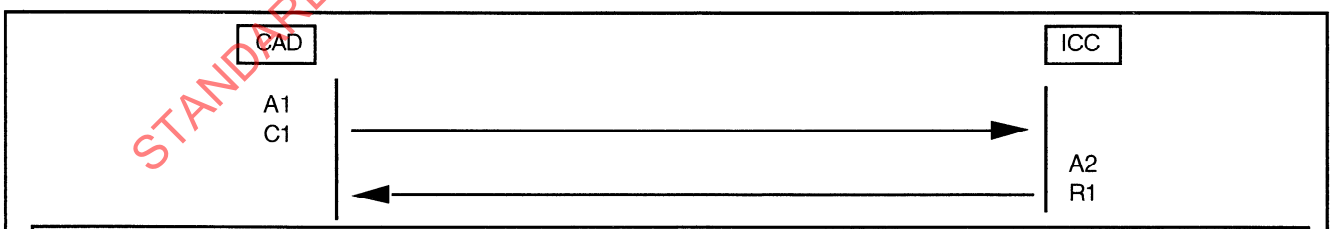
6.5.3.2 ADF choice and selection

The cardholder determines the ADF to be used and communicates the choice to the CAD.

The CAD sends a SELECT_FILE command to the ICC, giving the required Application ID of the DF supporting the ADF. The CAD may also request that File Control Information to be returned. According to ISO/IEC 7816-4, the ICC sets the current file to the selected DF. Subsequent access to EFs should be performed implicitly using the short EF identifier in the commands.

6.5.3.3 Decision

The CAD analyses the status conditions and optionally the File Control Information returned from the ICC. If there is no error condition, the CAD may issue a GET_PROCESSING_OPTIONS command in order to locate the data to be used. If there is no error condition, the CAD may process the next function.



Reference	Description	Parameters and data
A1	Acquisition of verification data	
C1	VERIFY	Verification data
A2	Check verification data	
R1		Status

Table 4 - Cardholder verification by the ICC

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

6.6 Transaction authorisation - decision made by the CAD

This subclause describes how transaction authorisation is carried out, where it is done by the CAD. Subclause E.2 in annex E describes how it is carried out, when it is done by the ICC.

6.6.1 Purpose

To process a request for approval for a transaction where the decision is made by the CAD.

6.6.2 Description

The authorisation function consists of obtaining the data necessary to perform the authorisation decision and determining whether or not to approve the request.

The CAD acquires the data, as defined by the application supplier, necessary to perform the transaction.

The CAD issues a READ to the ICC to retrieve application specific data necessary to enable it to make the authorisation decision. The specific application may require multiple READs in order to acquire all the required information.

The ICC informs the CAD of the Status of the request (completed successfully, not completed, unable to perform requested action) and, if available, the requested data.

The CAD acquires the transaction data and prompts for cardholder acceptance of the transaction amount if appropriate. The CAD then performs the authorisation using the transaction data, the cardholder acceptance response and the authorisation parameters provided by the ICC.

The results of the authorisation may be :

1) Approved

2) Denied

3) On-line authorisation required

4) Voice referral required

If approved, the CAD informs the user that the authorisation has been approved. If the application supplier, as an option, requires a confirmation (from the user) that the transaction has been completed, then this shall be done before proceeding with the next function.

If approved or denied, the CAD may inform the user and/or the ICC of the result.

6.6.3 Process flow (see table 6)

6.6.3.1 Determination of available ICC authorisation parameters

The CAD retrieves the necessary information using a READ to the ICC to determine the application specific data necessary to carry out an authorisation request.

The ICC responds by sending that data, if available.

The CAD then selects the ICC authorisation parameters that apply to the transaction.

The CAD acquires the specific data elements of the transaction through user entry. This task is accomplished by the CAD and requires no communication with the ICC.

6.6.3.2 Determination of cardholder acceptance

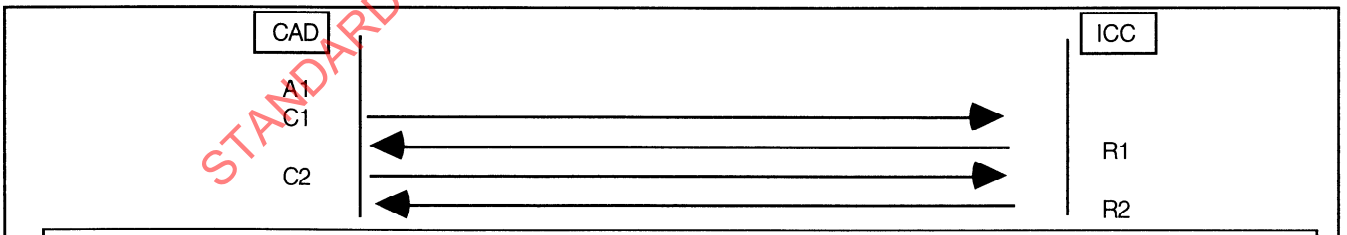
This task is accomplished by the CAD and requires no communication with the ICC.

6.6.3.3 CAD processes authorisation request

Depending on the authorisation parameters obtained by the CAD, the authorisation request is either processed off-line in the CAD or transmitted on-line to the Application Supplier or its agent.

The following are some examples of when an authorisation request may be routed on-line :

Off-line authorisation not allowed :
- by the CAD
- by the ICC



Reference	Description	Parameters and data
A1	Determination of selection parameters of available ADF(s) ; the cardholder chooses a service and an application id (#321) is found.	
C1	SELECT_FILE	#321
R1		
C2	GET_PROCESSING_OPTIONS	
R2		

Table 5 - ADF selection

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

- by the transaction type.

Transaction amount exceeds CAD off-line limit
Transaction is randomly selected
Another transaction for this card within the last *n* transactions
Too many off-line transactions
Too many off-line transactions since last on-line

When a transaction is denied, the CAD may send a GENERATE_TCC command to the ICC with the relevant data elements, requesting the creation of a Transaction Denial Code (#419).

6.6.3.4 Decision and final processing

The CAD may inform the ICC whether the transaction has been approved or denied. If the application supplier, as an option, requires a confirmation response from the ICC to the CAD, this shall be done before proceeding to the next function. This confirmation response informs the CAD that the transaction has been completed. The CAD updates (by UPDATE_RECORD as specified in subclause 4.8.x) the relevant data elements in the ICC (e.g. #403, #405, #407)

If the denial response includes indications to deactivate certain applications within the card, this shall be done immediately according to ISO 10202-1.

6.7 Transaction recording

6.7.1 Purpose

To record the details of the transaction in the ICC.

6.7.2 Description

If requested by the application supplier, this function shall be executed after any required authorisation function has been performed.

The recording function is performed by an APPEND_RECORD sent by the CAD to instruct the ICC to record the transaction. The specific information to be recorded is determined by the application as specified by the "data elements for logging" (#503).

The ICC replies to the command with a Response message that contains a Status Code (successful or unsuccessful completion, unable to perform command) according to ISO/IEC 7816-4.

The CAD may include the Authorisation code (#514) provided in an on-line interface as specified by ISO 8583.

The recording of the Authorisation code (#514) and how or if it will be used in the generation of a TCC is determined by the application supplier and is not governed by this International Standard except for its inclusion (or not) in the "data elements for logging" (#503).

6.7.3 Process flow (see table 7)

6.7.3.1 Parameter determination

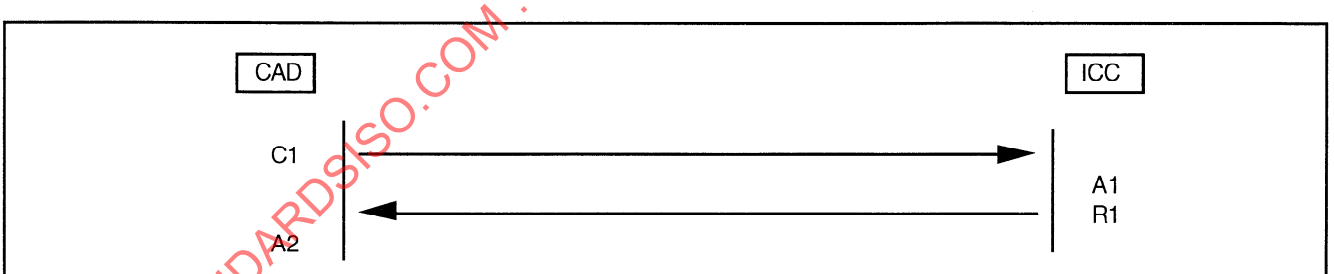
The CAD shall read the "transaction log indicator" (#501), "data elements for logging" (#503) and the "file-id for logging" (#502) to determine if transaction logging is required. The CAD shall then implicitly select the cyclic file for logging.

6.7.3.2 Record transaction

If it is required, the data elements specified in "data elements for logging" (#503) shall be written in the log file using an APPEND_RECORD command.

6.7.3.3 Terminate transaction recording

If the status condition indicates that the transaction recording process in the ICC was successful, the transaction recording is terminated.



Reference	Description	Parameters and data
C1	READ	Application defined parameters
A1	ICC accesses data and builds a response message	
R1	Response message provides status and requested data elements	Completion status code ; Application parameters :
A2	The CAD may use the GENERATE_TCC command to create an On-line Authorisation Code (#420) to be sent to the Application Supplier	
C2	UPDATE (optional)	Data elements #403, 405, 407 and ...
R2	Response message	

Table 6 - Transaction Authorisation by CAD

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

6.8 Transaction Cryptogram Code (TCC) generation

This subclause describes how TCC generation is carried out.

6.8.1 Purpose

To provide the card issuer or the application supplier with proof that the card and the cardholder (if a cardholder verification has taken place in the ICC) were party to the transaction.

6.8.2 Description

The CAD acquires the data, as defined by the application supplier, necessary to perform the TCC generation.

The CAD then sends a GENERATE_TCC command to the ICC.

The ICC performs the computation and creates a TCC (#418 or #419 or #420 or #421).

It then sends the TCC to the CAD.

6.8.3 Process flow (see table 8)

The CAD reads tag '5C', followed either by tag '8C' or by tag '8D', followed by a lists of tags.

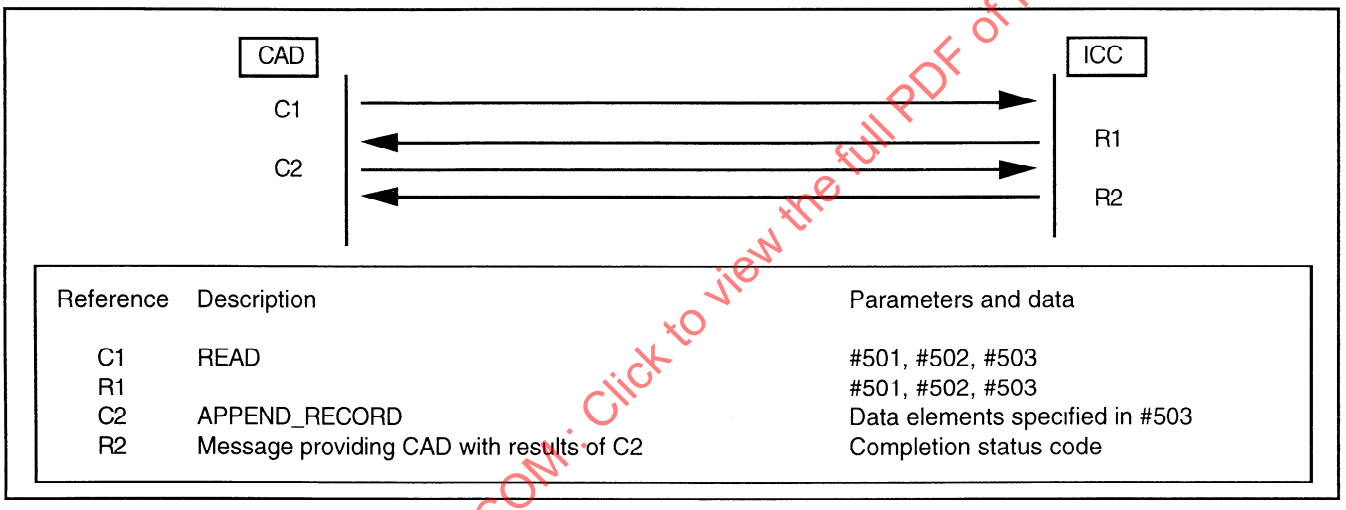
The lists of tags, which follow '8C' or '8D', defined by the Application Supplier, identify data elements required by the ICC to be sent in the data field of the GENERATE_TCC command.

The values of the tags are provided by the CAD, e.g. transaction date, transaction amount, etc.

The CAD sends a GENERATE_TCC command with the required data in the same order as read from the tag list.

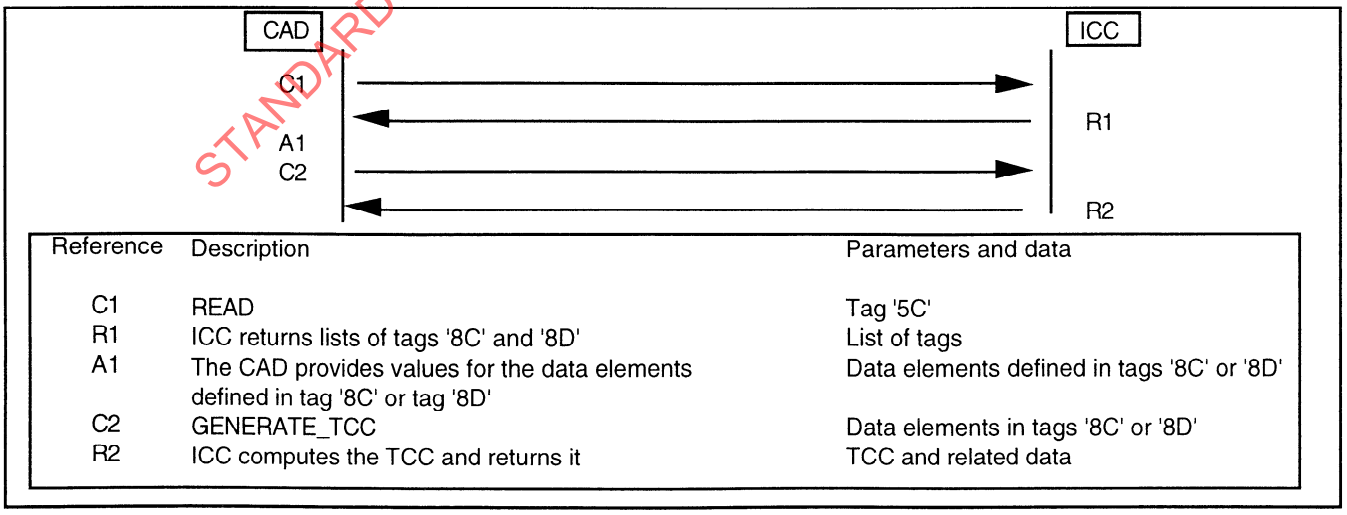
The ICC computes the TCC according to the algorithm defined by the Application Supplier.

The TCC may contain ICC internal data elements, e.g. application transaction counter (#415).



Reference	Description	Parameters and data
C1	READ	#501, #502, #503
R1		#501, #502, #503
C2	APPEND_RECORD	Data elements specified in #503
R2	Message providing CAD with results of C2	Completion status code

Table 7 - Transaction recording



Reference	Description	Parameters and data
C1	READ	Tag '5C'
R1	ICC returns lists of tags '8C' and '8D'	List of tags
A1	The CAD provides values for the data elements defined in tag '8C' or tag '8D'	Data elements defined in tags '8C' or '8D'
C2	GENERATE_TCC	Data elements in tags '8C' or '8D'
R2	ICC computes the TCC and returns it	TCC and related data

Table 8 - Transaction Cryptogram Code (TCC) generation

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

6.9 Transaction termination

6.9.1 Purpose

To terminate the transaction and, optionally, to deactivate the file at the request of the application supplier

6.9.2 Description

The Transaction termination function is performed when the transaction is completed or aborted for any reason.

At the request of the application supplier, the CAD may order the ICC to deactivate the current file. After that point, the transaction is terminated. Either a new transaction shall be initiated or the session shall be terminated.

6.9.3 Process flow (see table 9)

6.9.3.1 Deactivate the file (optional)

At the request of the application supplier, this function shall include a command to temporarily deny access to a file. This will be done according to the DEACTIVATE_FILE command, described in subclause 7.1 of this International Standard.

6.9.3.2 Terminate the transaction

There are two possibilities, based on the value of the status received after the last processed function.

When the CAD has detected no error condition, it shall either initiate a new financial transaction or the session shall be terminated.

When an error has occurred, the CAD shall update the appropriate parameters according to the function denied and the value of the error code. Either a new transaction shall be initiated or the session shall be terminated.

7 Messages (commands and responses)

The following commands and their corresponding responses are described :

- DEACTIVATE_FILE
- GENERATE_TCC
- GET_PROCESSING_OPTIONS

The impact of secure messaging on the message structure is not described in this clause. The list of error and warning conditions given in each subclause 7.x.5 is not exhaustive.

7.1 DEACTIVATE_FILE

7.1.1 Definition and scope

To temporarily deny access to a CDF or an ADF (either at card level or at Dedicated File level).
The command may refer to any file in the ICC.

7.1.2 Conditional usage and security

The DEACTIVATE_FILE command is issued by the CAD under the direct control of the provider of the file or his agent.

The file to be deactivated shall be the current file.

A previous successful EXTERNAL_AUTHENTICATE command may have been required.

The security status remains unchanged. The current file is temporarily locked.

7.1.3 Command message

CLA	h'Bx'
INS	h'04'
P1	h'00'
P2	h'00'
L_c field	Length of the cryptogram, or 0 if no data field
Data field	Cryptogram or empty
L_e field	Empty

Table 10 - Coding of the DEACTIVATE_FILE command

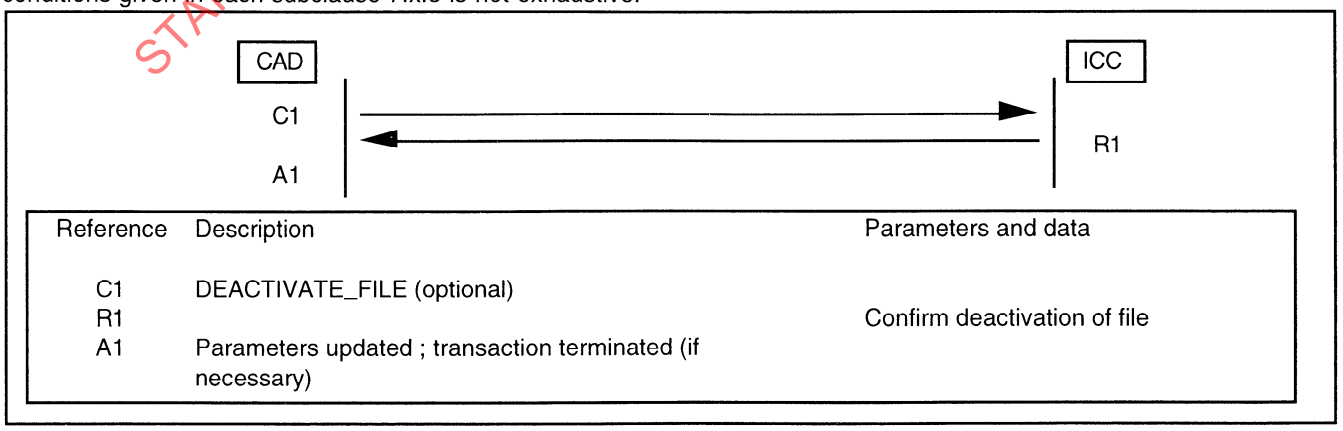
When the file requires a cryptogram, it shall be present in data field, and the ICC shall process it.

The cryptogram provides a mechanism to authenticate the initiator of the command.

7.1.4 Response message

Data field	Empty
SW1-SW2	Status bytes

Table 11 - Coding of the DEACTIVATE_FILE response



Reference	Description	Parameters and data
C1	DEACTIVATE_FILE (optional)	
R1		Confirm deactivation of file
A1	Parameters updated ; transaction terminated (if necessary)	

Table 9 - Transaction termination

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

7.1.5 Status conditions

The following specific warning condition may occur :

- SW1 = '9E' SW2 = '81' cryptogram provided but not required,

The following specific error conditions may occur :

- SW1 = '67' SW2 = '00' wrong length,
- SW1 = '69' SW2 = '85' conditions of use not satisfied (the command is not allowed in the context),
- SW1 = '6A' SW2 = '86' incorrect parameters P1-P2.

7.2 GENERATE_TCC

7.2.1 Definition and scope

At the discretion of the application supplier, a Transaction Cryptogram Code (TCC) may be generated by the ICC to prove to the card issuer or application supplier the genuineness and source of certain transaction information and the completion of the transaction.

The response shall include the TCC Information Data (#416), Application Transaction Counter (ATC - data element #415), TCC, and optionally Issuer Application Data (#417).

The TCC may be a Transaction Certificate (TC - data element #418), a Transaction Denial Code (TDC - data element #419), an On-line Authorisation Code (OAC - data element #420), or a Referral Code (RC - data element #421).

NOTE: The value of the current Application Transaction Counter (ATC) in the ICC should be used in the computation of the TCC.

7.2.2 Conditional usage and security

The ICC shall permit a maximum of two GENERATE_TCC commands to be performed during a session.

Depending upon the security attributes, the command may require a previous successful VERIFY command.

7.2.3 Command message

CLA	h'Bx'
INS	h'AE'
P1	Reference control.
P2	h'00'.
L_c field	Number of bytes of the data field
Data field	Transaction-related data to be used to compute the TCC
L_e field	h'0B' to h'2B'

Table 12 - Coding of the GENERATE_TCC command

The reference control parameter of the GENERATE_TCC command is coded as shown in Table 13:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							TDC
0	1							TC
1	0							OAC
1	1							RFU
		x	x	x	x	x	x	RFU

Table 13 - GENERATE_TCC Reference Control Parameter

NOTE : Data passed to the ICC in the command message are used for card risk management and/or in the computation of the TCC.

7.2.4 Response message

The response message contains the concatenation in the following order and without delimiters (tag and length) of the value fields of the following data objects, followed by the two bytes of the processing status:

- TCC Information Data, #416 - 1 byte
- ATC, #415 - 2 bytes
- TCC, 8 bytes
- (optional) Issuer Application Data, #417 - up to 32 bytes
- SW1 - SW2

The TCC Information Data returned by the GENERATE_TCC response message is coded according to Table 14:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							TDC
0	1							TC
1	0							OAC
1	1							RC
		x						RFU
			x	x	x	x	x	Issuer Proprietary

Table 14 - Coding of TCC Information Data

7.2.5 Status conditions

A successful execution of the command is coded by '90' '00'.

The following specific warning condition may occur.

SW1 = h'62', SW2 = h'81': part of returned data may be corrupted

The following specific error conditions may occur.

SW1 = h'64', SW2 = h'00': State of non-volatile memory unchanged
SW1 = h'67', SW2 = h'00': Lc incorrect or Le not present
SW1 = h'68', SW2 = h'82': Secure messaging not supported
SW1 = h'69', SW2 = h'85': Condition of use not satisfied
SW1 = h'6A', SW2 = h'80': Invalid parameter in data field
SW1 = h'6A', SW2 = h'86': Incorrect P1 P2

7.3 GET_PROCESSING_OPTIONS

7.3.1 Definition and scope

This command is used to obtain information describing the

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

location of a list of data specific to the application.

7.3.2 Conditional usage and security

A previous successful completion of a SELECT_FILE command of the ADF shall have been performed. The security status remains unchanged.

7.3.3 Command message

CLA	h'Bx'
INS	h'A8'
P1	h'00'
P2	h'00'.
L_c field	Number of bytes of the data field
Data field	Empty or Proprietary CAD environment related data
L_e field	variable

Table 15 - Coding of the GET_PROCESSING_OPTIONS command

7.3.4 Response message

Data field	TLV coded Application interchange profile (#322) and application data list (#323)
SW1-SW2	Status bytes

Table 16 - Coding of the GET_PROCESSING_OPTIONS response

7.3.5 Status conditions

A successful execution of the command is coded by '90' '00'.

The following specific warning condition may occur:

SW1 = h'62', SW2 = h'81': part of returned data may be corrupted.

The following specific error conditions may occur :

SW1 = h'64', SW2 = h'00': State of non-volatile memory unchanged
SW1 = h'67', SW2 = h'00': Wrong length
SW1 = h'69', SW2 = h'85': Condition of use not satisfied
SW1 = h'6A', SW2 = h'81': Function not supported.

8 Data elements and their organisation

8.1 Data elements

NOTE : *Unassigned values in Content are reserved to be further assigned by ISO/TC 68.*

The following data elements are logically arranged to provide better understanding. However, the Identifier attached to each data element is not used as the code for referring to the data element.

8.1.1 Card specific data

8.1.1.1 Data element 101 : IC manufacturer identifier

Purpose : To uniquely identify the manufacturer of the IC.

Format : 1 byte b, possibly expandable.

Content : Defined and registered by ISO/IEC JTC1/SC17 secretariat.

8.1.1.2 Data element 102 : Manufacturer's IC type identifier

Purpose : To identify for a given manufacturer each IC design and/or batch of ICs produced.

Format : 2 bytes b.

Content : To be defined by the IC manufacturer.

8.1.1.3 Data element 103 : Embedder/IC assembler Identifier

Purpose : To identify the organisation which combines the IC Card assembly and the plastic card.

Format : 5 characters an in the format CCEEA.

Content : CC-2 alphabetic country code of the embedder as defined in ISO 3166.
EE-2 alphanumeric characters based on the name of the embedder to be defined by each national body.
A-1 alphanumeric character for other purposes, e.g. to identify the IC assembler.

NOTE : This data element is for private use and is not registered by ISO.

8.1.1.4 Data element 104 : (deleted)

8.1.1.5 Data element 105 : IC serial number

Purpose : To uniquely identify IC components produced by the manufacturer.
Format : 4 bytes b.

Content : To be defined by the IC component manufacturer.

8.1.1.6 Data element 106 : (deleted)

8.1.1.7 Data element 107 : Key identifier.

Purpose : To uniquely identify the key used during a cryptographic process.

Format : 1 byte b.

Content : To be defined by the Application Supplier.

8.1.1.8 Data element 108 : (deleted)

8.1.2 Cardholder and Card Issuer specific data

8.1.2.1 Data element 201 : Card personaliser identifier

Purpose : To identify the personaliser of the card (see ISO 10202-1).

Format : 1 byte b.

Content : To be defined by the Card Issuer.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

8.1.2.2 Data element 202 : Cardholder name

Purpose : To indicate the name of the cardholder.

Format : 2 to 26 characters ans.

Content : see ISO 7813 Subclause 9.1.2 field NM.

8.1.2.3 Data element 203 : Cardholder name extended

Purpose : To extend the name of the cardholder.

Format : up to 26 characters ans.

Content : Extension of the previous data element.

8.1.2.4 Data element 204 : Language preferences

Purpose : To indicate up to 4 preferred languages for the cardholder.

Format : Up to 4 fields of 2 characters a.

Content : see ISO 639. The fields shall be in order of preference, the most preferred language first.

8.1.2.5 Data element 205 : (deleted)

8.1.2.6 Data element 206 : CDF activator identifier

Purpose : To uniquely identify the activator of the CDF, when taken in conjunction with the Cardholder Identification number of the CDF (see Subclause 8.1.3.5).

Format : 4 digits n.

Content : To be defined by the Card Issuer.

8.1.2.7 Data element 207 : CDF activator serial number

Purpose : To uniquely identify, for a given CDF activator, the activated CDF.

Format : 6 digits n.

Content : To be defined by the CDF activator.

8.1.2.8 Data element 208 : Card effective date

Purpose : To identify the date of activation.

Format : 6 digits n in the format YYMMDD.

Content : YY-2 digits to signify the year
MM-2 digits to signify the month
DD-2 digits to signify the day.

8.1.2.9 Data element 209 : Track 1

Purpose : To contain the magnetic stripe data of track 1, when present in the card. However, the discretionary data may be different between the magnetic stripe data and the ICC.

Format : Up to 76 characters ans.

Content : As specified in ISO/IEC 7816-6.

8.1.2.10 Data element 210 : Track 2

Purpose : To contain the magnetic stripe data of track 2, when present in the card. However, the discretionary data may be different between the magnetic stripe data and the ICC.

Format : Up to 37 digits ns.

Content : As specified in ISO/IEC 7816-6.

8.1.2.11 Data element 211 : Track 3

Purpose : To contain the magnetic stripe data of track 3, when present in the card.

Format : Up to 104 digits ns.

Content : The information, encoded on track 3 of the magnetic stripe as defined in ISO 4909, including field separators.

8.1.2.12 Data element 212 : Card Interchange profile

Purpose : To describe the capabilities of the ICC to perform an interchange transaction.

Format : 2 or 3 bytes b.

Content : In the first byte, assignment is :

b1	one-step static ICC authentication available
b2	two-step static ICC authentication available
b3	dynamic ICC authentication available (symmetric)
b4	dynamic ICC authentication available (asymmetric)
b5	CAD authentication available
b6	cardholder verification by the ICC available
b7	transaction recording available
b8	TCC generation available.

When the bit = 0, the function is not supported ;
when the bit = 1, the function is supported.

The other bytes are RFU.

8.1.2.13 Data element 213 : Address

Purpose : To indicate the cardholder address.

Format : Up to 192 bytes.

Content : Defined by the cardholder.

8.1.2.14 Data element 214 : Date of birth

Purpose : To provide the date of birth of the cardholder.

Format : 8 digits n.

Content : YYYYMMDD.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

8.1.2.15 Data element 215 : Special user requirements

Purpose : To provide specific requirements of the cardholder to the CAD.

Format : Up to 10 bytes.

Content : Contains at least a data object denoting a responsible authority and a data object by which this authority indicates the requirements of an user, possibly related to a disability.

8.1.2.16 Data element 216 (deleted)

8.1.2.17 Data element 217 : Card expiry date

Purpose : To indicate the date after which the card ceases to be valid.

Format : 4 digits n in the format YYMM.

Content : YY-2 digits to signify the year when the card ceases to be valid.
MM-2 digits, as the numeric sequence of the month within the year. The card ceases to be valid on the last day of the month specified.
NOTE : The value '0001' follows '9912'.

8.1.3 Application Supplier specific data

NOTE : All of the following data elements can apply to the CDF as well as to any ADF.

8.1.3.1 Data element 301 : (deleted)

8.1.3.2 Data element 302 : (deleted)

8.1.3.3 Data element 303 : (deleted)

8.1.3.4 Data element 304 : Application label

Purpose : To permit application selection using a term chosen by the cardholder when the application is allocated.

Format : Up to 16 characters an.

Content : As defined in ISO/IEC 7816-5, subclause 3.1.

8.1.3.5 Data element 305 : Cardholder identification number

Purpose : To identify the Card issuer or Application Supplier and the related individual account of the cardholder

Format : up to 19 digits n.

Content : see ISO 7812, subclause 3.1. Note that the check digit is included

8.1.3.6 Data element 306 : (deleted)

8.1.3.7 Data element 307 : Card sequence number

Purpose : To distinguish between separate applications (issued concurrently or consecutively) with the same cardholder identification number.

Format : 2 digits n.

Content : At Application Supplier's discretion.

8.1.3.8 Data element 308 : Country code

Purpose : To identify a country specified by the Card Issuer or the Application Supplier.

Format : 3 digits n.

Content : see ISO 3166.

8.1.3.9 Data element 309 : Application effective date

Purpose : To indicate the day of the month in the year when the current ADF becomes valid (i.e. available for transactions).

Format : 6 digits n in the format YYMMDD.

Content : YY-2 digits to signify the year when the card or the ADF becomes valid.
MM-2 digits, as the numeric sequence of the month within the year.
DD-2 digits, as the numeric sequence of the day within the month.
Value '000000' = valid as soon as delivered to the cardholder.
NOTE : The value '000101' follows '991231'.

8.1.3.10 Data element 310 : Application expiry date

Purpose : To indicate the date after which the current ADF ceases to be valid.

Format : 4 digits n in the format YYMM.

Content : YY-2 digits to signify the year when the current ADF ceases to be valid.
MM-2 digits, as the numeric sequence of the month within the year. The current ADF ceases to be valid on the last day of the month specified.
NOTE : The value '0001' follows '9912'.

8.1.3.11 Data element 311 :Discretionary data 1

Purpose : To contain discretionary data meaningful to the Application Supplier.

Format : Variable length, up to 252 characters binary.

Content : At the Application Supplier's discretion.

8.1.3.12 Data element 312 :Discretionary data 2

Purpose : To contain discretionary data meaningful to the Application Supplier.

Format : Variable length, up to 252 characters binary.

Content : At the Application Supplier's discretion.

8.1.3.13 Data element 313 :Discretionary data 3

Purpose : To contain discretionary data meaningful to the

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

Application Supplier.

Format : Variable length, up to 252 characters binary.

Content : At the Application Supplier's discretion.

8.1.3.14 Data element 314 :Discretionary data 4

Purpose : To contain discretionary data meaningful to the Application Supplier.

Format : Variable length, up to 252 characters binary.

Content : At the Application Supplier's discretion.

8.1.3.15 Data element 315 : Service code

Purpose : To indicate restrictions on the use of the application supported by the current file (CDF or ADF).

Format : 3 digits n.

Content : see ISO 7813 subclause 9.1.2 as amended in DAM 1.

8.1.3.16 Data element 316 : Currency code

Purpose : To denote the currency for the application supported by the current file (CDF or ADF).

Format : 3 digits n.

Content : see ISO 4217.

8.1.3.17 Data element 317 : Currency exponent

Purpose : To determine the base value of amounts for the application supported by the current file (CDF or ADF).

Format : 1 digit n.

Content : see ISO 4909, field 7.

NOTE : This field is used with the data elements in subclauses 8.1.4.1, 8.1.4.6, 8.1.4.7, 8.1.4.8, 8.1.4.11, 8.1.4.12.

8.1.3.18 Data element 318 : Cardholder PIN reference data

Purpose : To allow for cardholder PIN verification.

Format : Used for the ID method 01 (PIN). The format is variable length 4 to 12 characters n (see also ISO 9564).

Content : The value used to check the PIN entered by the cardholder.

8.1.3.19 Data element 319 : Cardholder biometric reference data

Purpose : To allow for cardholder biometric verification.

Format : Variable length.

Content : Biometric information for verifying cardholder.

8.1.3.20 Data element 320 : (deleted)

8.1.3.21 Data element 321 : Application Identifier

Purpose : To identify an application in a card according to ISO/IEC 7816-5.

Format : 5-16 bytes b.

Content : As defined in ISO/IEC 7816-5.

8.1.3.22 Data element 322 : Application Interchange Profile

Purpose : To describe the capabilities of the application to perform an interchange transaction.

Format : 2 bytes b.

Content : To be defined by the Application Supplier.

8.1.3.23 Data element 323 : Application data list

Purpose : To describe the data retrieved in the response to a GET_PROCESSING_OPTIONS command.

Format : 128 bytes b.

Content : To be defined by the Application Supplier.

8.1.4 Authorisation data

8.1.4.1 Data element 401 : Floor limit

Purpose : To specify the cardholder upper limit at which transactions can take place off-line for this application.

Format : 7 digits n.

Content : Amount in the currency of the current file, modified by the currency exponent (see subclause 8.1.3.17). To be specified by the Application Supplier.

8.1.4.2 Data element 402 : Maximum number of off-line authorisations

Purpose : To specify the maximum number of off-line authorisations which can be carried out consecutively for this application (without an authorisation on-line from the Application Supplier).

Format : 2 digits n.

Content : Value supplied by the Application Supplier. 00 = always on-line
01-98 = the number of consecutive off-line authorisations as specified by the application supplier
99 = no requirement to go on-line.

8.1.4.3 Data element 403 : Number of consecutively performed off-line authorisations

Purpose : To provide the number of off-line authorisations since the latest successful on-line authorisation.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

Format : 2 digits n.

Content : A counter reset after each successful on-line authorisation.

8.1.4.4 Data element 404 : Maximum consecutive days off-line

Purpose : To specify the maximum number of consecutive days during which off-line transactions can be carried out without an authorisation on-line from the Application Supplier.
Format : 3 digits n.

Content : Value supplied by the Application Supplier. 000 = always on-line
001-998 = the maximum number of days during which transactions can be carried out off-line (as in subclause 8.1.4.2)
999 = no requirement to go on-line.

8.1.4.5 Data element 405 : Date latest on-line authorisation

Purpose : To provide the date of the last authorisation on-line from the Application Supplier.

Format : 6 digits n in the format YYMMDD.

Content : YY-2 digits to signify the year
MM-2 digits to signify the month
DD-2 digits to signify the day.

8.1.4.6 Data element 406 : Maximum total off-line amount

Purpose : To provide the maximum total amount that can be authorised off-line (i.e. without an authorisation on-line from the Application Supplier).

Format : 8 digits n.
Content : Amount in the currency of the current file, modified by the currency exponent (see subclause 8.1.3.17). To be specified by the Application Supplier.
99999999 = no requirement to go on-line.

8.1.4.7 Data element 407 : Total off-line amount

Purpose : To provide the total amount rounded as appropriate that has been authorised off-line since the latest on-line authorisation.

Format : 8 digits n.

Content : Amount in the currency of the current file, modified by the currency exponent (see subclause 8.1.3.17).

8.1.4.8 Data element 408 : Revolving credit limit

Purpose : To specify the maximum total amount that may be authorised during a credit cycle. Used to reset the amount remaining (see subclause 8.1.4.11) at the start of a new cycle.

Format : 8 digits n.

Content : To be provided by the Application Supplier. Amount in the currency of the current file, modified by the currency exponent (see subclause 8.1.3.17).

8.1.4.9 Data element 409 : Revolving credit cycle length

Purpose : To denote the period of time during which the accumulated sum of all transactions shall not exceed the revolving credit limit.

Format : 2 digits n.
Content : To be provided by the Application Supplier. See ISO 4909 subclause 8.11.

8.1.4.10 Data element 410 : Revolving credit cycle begin

Purpose : To denote the date at which a new cycle period begins.

Format : 5 digits n in the format YYDDD.

Content : To be provided by the Application Supplier.
YY-2 digits to signify the year.
DDD-3 digits to signify the day.
As specified in ISO 4909 (field 10).
The field shall be updated to the current date when the value of this field plus the value of the revolving credit cycle length (8.1.4.9) is less than or equal to the current date, unless the value of the revolving credit cycle length (8.1.4.9) is set in the range 80-99.

8.1.4.11 Data element 411 : Amount remaining this cycle

Purpose : To denote the remaining available balance of the revolving credit limit for the current cycle period.

Format : 8 digits n.

Content : Amount in the currency of the current file, modified by the currency exponent (see subclause 8.1.3.17). On the first use after the commencement of each new cycle period, this field shall be reset to the value shown in the revolving credit limit (8.1.4.8). Thereafter it shall contain the amount remaining this cycle.

8.1.4.12 Data element 412 : Remaining credit

Purpose : To indicate the amount of credit still available to the cardholder.

Format : 8 digits n.

Content : Amount in the currency of the current file, modified by the file currency exponent (see subclause 8.1.3.17). To be updated with information from the Application Supplier when the authorisation is done on-line ; between on-line authorisations, the value is modified by the value of the transaction.

8.1.4.13 Data element 413 : Cash/Debit Account Amount remaining

Purpose : To indicate the amount that is still available to the cardholder to obtain cash or buy goods or services.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

Format : 12 digits n.

Content : Amount in the minor unit of the currency of the current file ; it is modified after each transaction.

8.1.4.14 Data element 414 : Transaction authorising capability indicator

Purpose : To indicate whether the ICC is capable of authorising the current transaction.

Format : 1 byte b.

Content : 0 = ICC can authorise transaction
1 = ICC cannot authorise transaction
2-9 for Application Supplier use
other values = reserved for ISO/TC 68.

8.1.4.15 Data element 415 : Application transaction counter

Purpose : To uniquely identify each transaction performed within this file.

Format : 2 bytes b.

Content : Sequential number related to the current file.

8.1.4.16 Data element 416 : TCC information data

Purpose : To indicate the type of TCC returned by the card.

Format : 1 byte b.

Content : See table 14.

8.1.4.17 Data element 417 : Issuer application data

Purpose : To provide proprietary application data for transmission to the issuer in an on-line transaction.

Format : up to 32 bytes b.

Content : Proprietary application related data provided by the issuer.

8.1.4.18 Data element 418 : Transaction certificate (TC)

Purpose : To provide a certificate, denoting successful completion of the transaction, generated by the ICC.

Format : 8 bytes b.

Content : A cryptogram generated by the card.

8.1.4.19 Data element 419 : Transaction Denial Code (TDC)

Purpose : To provide a certificate, denoting denial of the transaction, generated by the ICC.

Format : 8 bytes b.

Content : A cryptogram generated by the card.

8.1.4.20 Data element 420 : On-line Authorisation Code (OAC)

Purpose : To provide a certificate to be transmitted to the issuer during on-line authorisation.

Format : 8 bytes b.

Content : A cryptogram generated by the card.

8.1.4.21 Data element 421 : Referral Code (RC)

Purpose : To request a voice referral of the transaction.

Format : 8 bytes b.

Content : A cryptogram generated by the card.

8.1.4.22 Data element 422 : Data object list 1

Purpose : To identify data elements required for the data field of the GENERATE_TCC command.

Format : up to252 bytes b.

Content : A list of tags.

8.1.4.23 Data element 423 : Data object list 2

Purpose : To identify data elements required for the data field of the GENERATE_TCC command.

Format : up to 252 bytes b.

Content : A list of tags.

8.1.5 Data elements for logging

8.1.5.1 Data element 501 : Transaction log indicator

Purpose : To indicate if and how the transaction shall be logged.

Format : 1 digit n.

Content : To be provided by the Application Supplier. 0 = no logging
1 = logging, approved transaction only, according to parameters contained in the next two data elements.
2 = logging, approved and denied transactions, according to parameters contained in the next two data elements.
3-9 = reserved for ISO/TC 68.

8.1.5.2 Data element 502 : File ID for logging

Purpose : To indicate the file-id of the file within the application into which the transaction shall be logged.

Format : 2 bytes b.

Content : The File-id to which the transaction shall be logged (see subclause 8.1.3.1).

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

8.1.5.3 Data element 503 : Data elements for logging.

Purpose : To specify the tags of the data elements to be logged in the ICC for each transaction.

Format : variable.

Content : A tag list, as defined in ISO/IEC 7816-6, subclause 5.6.

8.1.5.4 Data element 504 : Transaction date

Purpose : To provide the date when the transaction took place.

Format : 6 digits n in the format YYMMDD.

Content : YY-2 digits to signify the year
MM-2 digits to signify the month
DD-2 digits to signify the day.

8.1.5.5 Data element 505 : Transaction time

Purpose : To provide the local time when the transaction took place.

Format : 6 digits n in the format HHMMSS.

Content : Local time in 24 hour format
HH-00-23, two digits to signify the hour
MM-00-59, two digits to signify the minutes
SS-00-59, two digits to signify the seconds.

8.1.5.6 Data element 506 : Card acceptor name and location

Purpose : To identify the card acceptor of the transaction and optionally the location.

Format : up to 40 characters an.

Content : Defined by the card acceptor.

8.1.5.7 Data element 507 (deleted)

8.1.5.8 Data element 508 : (deleted)

8.1.5.9 Data element 509 : Processing code

Purpose : To define the type of transaction.
Format : 6 digits n.
Content : digits 1-2 describe a specific transaction ; values are described in ISO 8583, subclause A.9.
digits 3-4 describe the account type affected for debits and inquiries, and the "from" account for transfers.
digits 5-6 describe the account type affected for credits and the "to" account for transfers.
Values for digits 3-6 are described in ISO 8583, subclause 8.1.3.8, except for value 6 in positions 3 and 5 which is allocated to "Electronic purse/wallet/token facility".

8.1.5.10 Data element 510 : Transaction amount (file currency)

Purpose : To provide the amount of the transaction in the currency of the current file.

Format : 12 digits n.

Content : The amount of the transaction in the minor unit of file currency.

8.1.5.11 Data element 511 : Transaction amount (original currency)

Purpose : To provide the amount of the transaction in the original currency, where different from the file currency.

Format : 12 digits n.

Content : The amount of the transaction in the minor unit of original currency.

8.1.5.12 Data element 512 : Original currency code

Purpose : To provide the original currency code of the transaction.

Format : 3 digits n.

Content : see ISO 4217.

8.1.5.13 Data element 513 : Transaction authorising source

Purpose : To identify the authoriser of the transaction.

Format : 1 byte b.

Content : Denotes the source(s) of the authorisation for the current transaction.
b8 = ICC
b7 = CAD
b6 = SAM
b5 = Acquirer
b4 = Card scheme
b3 = Application Supplier
b2 = Card Issuer
b1 = reserved for ISO/TC 68.

When the bit = 0, the function is not supported ;
when the bit = 1, the function is supported.

8.1.5.14 Data element 514 : Authorisation code

Purpose : To indicate the code used by the authoriser claiming that the transaction has been authorised.

Format : 6 digits an.

Content : In accordance with ISO 8583 (authorisation identification response). To be specified by the authoriser.

8.1.5.15 Data element 515 (deleted)

8.1.6 Authentication data

8.1.6.1 Data element 601 : Authentication algorithm identifier

Purpose : To uniquely identify the algorithm used for authentication.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

Format : 1 byte b.

Content : To be defined by the Application Supplier.

8.1.6.2 Data element 602 : Derivation parameter(s)

Purpose : To diversify the primary key into derived keys to be distributed.

Format : To be defined by TC68/SC6/WG7.

Content : To be defined by the Application Supplier

8.1.6.3 Data element 603 : Derivation function identifier

Purpose : To uniquely identify the function used for key derivation.

Format : 1 byte b.

Content : To be defined by the Application Supplier.

8.1.6.4 Data element 604 : CAD challenge

Purpose : To avoid replay of cryptographic computation.

Format : Up to 8 bytes b.

Content : Challenge generated by the CAD.

8.1.6.5 Data element 605 : Encipherment result

Purpose : To obtain the result of a cryptographic computation.

Format : Up to 252 bytes b.

Content : To be defined by the Application Supplier.

8.1.6.6 Data element 606 : ICC challenge

Purpose : To allow the ICC to verify a cryptogram.

Format : up to 16 bytes b.

Content : Challenge generated by a GET CHALLENGE command.

8.1.6.7 Data element 607 : External authentication related data

Purpose : To obtain the result of a cryptographic computation.

Format : Up to 8 bytes b.

Content : Data generated by the entity to be authenticated by the ICC.

8.1.6.8 Data element 608 : One step/key number

Purpose : To uniquely identify the key issuer (AID or RID or IIN) and the key identifier allocated by the key issuer, within the one-step authentication procedure.

Format : Up to 21 bytes b.

Content : Concatenation of ASN.1 objects :
- IIN or RID or AID of the key issuer, tag '4F',
- key number allocated by the issuer, tag '80'. The length is 1 byte.

8.1.6.9 Data element 609 : One step/signed data

Purpose : To be used within the one-step authentication procedure.

Format : Up to 128 bytes b.

Content : Defined by the Application Supplier.

8.1.6.10 Data element 610 : Two step/trusted third party key number

Purpose : To uniquely identify the trusted third party (AID or RID or IIN) and the key identifier allocated by the trusted third party, within the two-step authentication procedure.

Format : Up to 21 bytes b.

Content : Concatenation of ASN.1 objects :
- IIN or RID or AID of the key issuer, tag '4F',
- key number allocated by the trusted third party, tag '80'. The length is 1 byte.

8.1.6.11 Data element 611 : Two step/signed data #1

Purpose : To be used within the first step of the two-step authentication procedure.

Format : Up to 128 bytes b.

Content : Defined by the Application Supplier.

8.1.6.12 Data element 612 : Two step/public exponent #2

Purpose : To define the exponent to be used in connection with asymmetric algorithm related to the second step of the two-step authentication procedure.

Format : 1 byte b.

Content : Value of the exponent.

8.1.6.13 Data element 613 : Two step/signed data #2

Purpose : To be used within the second step of the two-step authentication procedure.

Format : Up to 128 bytes b.

Content : Defined by the Application Supplier.

8.2 Table of data elements

This table summarises identification, name, description, logical attributes (length, format and presence) related to each data element.

The data elements are identified by the same ID, whether they are in the CDF or in the ADF, which means that the

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

identification refers to the current file. These IDs are used to identify the data. Subclause 8.3 provides referencing methods to access data.

The length and format show the way application programs present and/or expect the data elements at the interface. This does not imply that the data are physically stored in the memory of the card in the manner depicted.

In the "length" column, the length of the data element is given in characters. In the case of binary format for a data element, the length is given in bytes. Where the presence of a data element is mandatory, the minimum length is 1. In the case of variable length, the minimum and maximum length is given.

In the column "M/O" (presence), M (= Mandatory) means that a request for that data element shall be answered positively; O (= Optional) means that a request for that data element may be answered with the response "not present".

Where a data element is shown as mandatory, this means that it shall be available from either the CDF or an ADF ; it is not mandatory for it to be present in both. When an element exists in the current ADF, it shall be used, rather than the value from the CDF. When the element does not exist in the current ADF, the value existing in the CDF shall be used.

In the column "R", P = public read access, N = no read access, C = conditional read access.
In the column "W", F = free write access, C = conditional write access, O = one time write access, I = only internal write access.
These protection attributes are those applicable during the transaction process.
C1 = forbidden during transaction process.
C2 = business agreement ; the agreement to be taken when 'C2' appears may apply differently from one data element to another but shall be identical within a given template.

8.2.1 Card specific data

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
101	IC manufacturer identifier	To uniquely identify the manufacturer of the IC.	1	b	M	P	C1
102	Manufacturer's IC type identifier	To identify for a given manufacturer each IC design and/or batch of ICs produced.	2	b	M	P	C1
103	Embedder/IC assembler Identifier	To identify the organisation which combines the IC Card assembly and the plastic card.	5	an	M	P	C1
105	IC serial number	To uniquely identify IC components produced by the manufacturer.	4	b	O	P	C1
107	Key identifier	To uniquely identify the key used during a cryptographic process.	1	b	O	P	C1

8.2.2 Cardholder and Card Issuer specific data

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
201	Card personaliser identifier	To identify the personaliser of the card.	1	b	M	P	C1
202	Cardholder name	To indicate the name of the cardholder.	2-26	ans	O	P	C1
203	Cardholder name extended	To extend the name of the cardholder.	-26	ans	O	P	C1
204	Language preferences	To indicate up to 4 preferred languages for the cardholder.	2-8	a	O	P	C1
206	CDF activator identifier	To uniquely identify the activator of the CDF, when taken in conjunction with the Cardholder Identification number of the CDF.	4	n	O	P	C1
207	CDF activator serial number	To uniquely identify, for a given CDF activator, the activated CDF.	6	n	O	P	C1
208	Card effective date	To identify the date of activation.	6	n	O	P	C1
209	Track 1	To contain the magnetic stripe data of track 1, when present in the card.	-76	ans	O	P	C1
210	Track 2	To contain the magnetic stripe data of track 2, when present in the card.	-37	ns	O	P	C1
211	Track 3	To contain the magnetic stripe data of track 3, when present in the card.	-104	ns	O	P	C1

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
212	Card Interchange profile	To describe the capabilities of the ICC to perform an interchange transaction.	2-3	b	M	P	C1
213	Address	To indicate the cardholder address.	-192	b	O	P	C1
214	Date of birth	To provide the date of birth of the cardholder.	8	n	O	P	C1
215	Special user requirements	To provide specific requirements of the cardholder to the CAD.	-10	b	O	P	C1
217	Card expiry date	To indicate the date after which the card ceases to be valid.	4	n	M	P	C1

8.2.3 Application Supplier specific data

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
304	Application label	To permit application selection using a term chosen by the cardholder when the application is allocated.	-12	an	O	P	C1
305	Cardholder identification number	To identify the Card issuer or Application Supplier and the related individual account of the cardholder.	-19	n	M	P	C1
307	Card sequence number	To distinguish between separate applications (issued concurrently or consecutively) with the same cardholder identification number.	2	n	O	P	C1
308	Country code	To identify a country specified by the Card Issuer or the Application Supplier.	3	n	O	P	C1
309	Application effective date	To indicate the day of the month in the year when the current ADF becomes valid (i.e. available for transactions).	6	n	O	P	C1
310	Application expiry date	To indicate the date after which the current ADF ceases to be valid.	4	n	O	P	C1
311	Discretionary data 1	To contain discretionary data meaningful to the Application Supplier.	-252	b	O	C2	C2
312	Discretionary data 2	To contain discretionary data meaningful to the Application Supplier.	-252	b	O	C2	C2
313	Discretionary data 3	To contain discretionary data meaningful to the Application Supplier.	-252	b	O	C2	C2
314	Discretionary data 4	To contain discretionary data meaningful to the Application Supplier.	-252	b	O	C2	C2
315	Service code	To indicate restrictions on the use of the application supported by the current file (CDF or ADF).	3	n	M	P	C1
316	Currency code	To denote the currency for the application supported by the current file (CDF or ADF).	3	n	O	P	C1
317	Currency exponent	To determine the base value of amounts for the application supported by the current file (CDF or ADF).	1	n	O	P	C1
318	Cardholder PIN reference data	To allow for cardholder PIN verification.	4-12	n	O	N	C1
319	Cardholder biometric reference data	To allow for cardholder biometric verification.		b	O	N	C1
321	Application Identifier	To identify an application in a card according to ISO/IEC 7816-5.	5-16	b	M	C2	C1
322	Application Interchange profile	To describe the capabilities of the application to perform an interchange transaction.	2	b	O	P	C1

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
323	Application data list	To describe the data retrieved in the response to a GET_PROCESSING_OPTIONS command.	-128	b	O	P	C1

8.2.4 Authorisation data

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
401	Floor limit	To specify the cardholder upper limit at which transactions can take place off-line for this application.	7	n	O	C2	C1
402	Maximum number of off-line authorisations	To specify the maximum number of off-line authorisations which can be carried out consecutively for this application.	2	n	O	C2	C1
403	Number of consecutively performed off-line authorisations	To provide the number of off-line authorisations since the latest successful on-line authorisation.	2	n	O	C2	C2
404	Maximum consecutive days off-line	To specify the maximum number of consecutive days during which off-line transactions can be carried out without an authorisation on-line from the Application Supplier.	3	n	O	C2	C1
405	Date latest on-line authorisation	To provide the date of the last authorisation on-line from the Application Supplier.	6	n	O	C2	C2
406	Maximum total off-line amount	To provide the maximum total amount that can be authorised off-line.	8	n	O	C2	C1
407	Total off-line amount	To provide the total amount rounded as appropriate that has been authorised off-line since the latest on-line authorisation.	8	n	O	C2	C2
408	Revolving credit limit	To specify the maximum total amount that may be authorised during a credit cycle.	8	n	O	C2	C1
409	Revolving credit cycle length	To denote the period of time during which the accumulated sum of all transactions shall not exceed the revolving credit limit.	2	n	O	C2	C1
410	Revolving credit cycle begin	To denote the date at which a new cycle period begins.	5	n	O	C2	C2
411	Amount remaining this cycle	To denote the remaining available balance of the revolving credit limit for the current cycle period.	8	n	O	C2	C2
412	Remaining credit	To indicate the amount of credit still available to the cardholder.	8	n	O	C2	C2
413	Cash/Debit Account Amount remaining	To indicate the amount that is still available to the cardholder to obtain cash or buy goods or services.	12	n	O	C2	C2
414	Transaction authorising capability indicator	To indicate whether the ICC is capable of authorising the current transaction.	1	b	O	C2	C2
415	Application Transaction counter	To uniquely identify each transaction performed within this file.	2	b	O	P	I
416	TCC information data	To indicate the type of TCC returned by the card.	1	b	O	P	I
417	Issuer application data	To provide proprietary application data for transmission to the issuer in an on-line transaction.	-32	b	O	P	I
418	Transaction certificate (TC)	To provide a certificate, denoting successful completion of the transaction, generated by the ICC.	8	b	O	C2	I
419	Transaction Denial Code (TDC)	To provide a certificate, denoting denial of the transaction, generated by the ICC.	8	b	O	C2	I

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
420	On-line Authorisation Code (OAC)	To provide a certificate to be transmitted to the issuer during on-line authorisation.	8	b	O	C2	I
421	Referral Code (RC)	To request a voice referral of the transaction.	8	b	O	C2	I
422	Data object list 1	To identify data elements required for the data field of the GENERATE_TCC command.	-252	b	O	C2	I
423	Data object list 2	To identify data elements required for the data field of the GENERATE_TCC command.	-252	b	O	C2	I

8.2.5 Data elements for logging

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
501	Transaction log indicator	To indicate if and how the transaction shall be logged.	1	n	O	C2	C1
502	File-id for logging	To indicate the file-id of the file within the application into which the transaction shall be logged.	2	b	O	C2	C1
503	Data elements for logging.	To specify the tags of the data elements to be logged in the ICC for each transaction.	n*2	b	O	C2	C1
504	Transaction date	To provide the date when the transaction took place.	6	n	O	C2	C2
505	Transaction time	To provide the local time when the transaction took place.	6	n	O	C2	C2
506	Card acceptor name and location	To identify the card acceptor of the transaction and optionally the location.	-40	an	O	C2	C2
509	Processing code	To define the type of transaction.	6	n	O	C2	C2
510	Transaction amount (file currency)	To provide the amount of the transaction in the currency of the current file.	12	n	O	C2	C2
511	Transaction amount (original currency)	To provide the amount of the transaction in the original currency, where different from the file currency.	12	n	O	C2	C2
512	Original currency code	To provide the original currency code of the transaction.	3	n	O	C2	C2
513	Transaction authorising source	To identify the authoriser of the transaction.	1	an	O	C2	C2
514	Authorisation code	To indicate the code used by the authoriser claiming that the transaction has been authorised.	6	an	O	C2	C2

8.2.6 Authentication data

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
601	Authentication algorithm identifier	To uniquely identify the algorithm used for authentication.	1	b	O	P	C1
602	Derivation parameter(s)	To diversify the primary key into derived keys to be distributed.			O	P	C1
603	Derivation function identifier	To uniquely identify the function used for key derivation.	1	b	O	P	C1
604	CAD challenge	To avoid replay of cryptographic computation.	-8	b	O	P	C1

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

ID	NAME	PURPOSE	LOGICAL ATTRIBUTES			Protection for transaction process	
			length	format	M/O	R	W
605	Encipherment result	To obtain the result of a cryptographic computation.	-252	b	O	P	C1
606	ICC challenge	To allow the ICC to verify a cryptogram.	-16	b	O	P	C1
607	External authentication related data	To obtain the result of a cryptographic computation.	-8	b	O	P	C1
608	One step/key number	To uniquely identify the key issuer (AID or RID or IIN) and the key identifier allocated by the key issuer, within the one-step authentication procedure.	-21	b	O	P	C1
609	One step/signed data	To be used within the one-step authentication procedure.	-128	b	O	P	C1
610	Two step/trusted third party key number	To uniquely identify the trusted third party (AID or RID or IIN) and the key identifier allocated by the trusted third party, within the two-step authentication procedure.	-21	b	O	P	C1
611	Two step/signed data #1	To be used within the first step of the two-step authentication procedure.	-128	b	O	P	C1
612	Two step/public exponent #2	To define the exponent to be used in connection with asymmetric algorithm related to the second step of the two-step authentication procedure.	1	b	O	P	C1
613	Two step/signed data #2	To be used within the second step of the two-step authentication procedure.	-128	b	O	P	C1

8.2.7 Algorithm and Key identifiers

Security related functions such as CDF/ADF_AUTHENTICATION or CAD_AUTHENTICATION require the reference to an algorithm and a key.

The algorithm identifier is not governed by this International Standard.

A key belongs to a set of keys (e.g. issuer keys, application supplier keys).

A key is defined :

- by the command to which it is associated (e.g. : INTERNAL AUTHENTICATE)
- or by the tags used in secure messaging (e.g. MAC),

If in an ICC system more than one key may be used with a specific command, the Key Number (associated with the command) denotes the key to be used for a specific Application in the ICC and the specific command.

The key number may be implicit (coded as key number 0) when there is only one key in the specific current file associated with the specific command.

8.3 Referencing of data elements

8.3.1 Management of data elements

The data elements defined in this International Standard are represented as Tag, Length, Value (TLV) elements coded as defined in ASN.1 notation (ISO 8824).

The following coding rules of the tags apply :

- data elements referenced by tags h'4X' or h'5X' shall have the same meaning wherever they are found and therefore are reserved for interindustry generic usage.

- tags h'6X' or h'7X' are used for constructed templates. A constructed template may be referenced as a record with the record ID being the tag.

- tags h'8X' or h'9X' are used to reference data elements with a meaning depending on the constructed template in which they appear.

8.3.2 Coding of data as seen at the interface

Numeric data shall use BCD coding with 2 digits per byte or 1 digit and 1 special character (-).

Alphanumeric data shall be coded in ASCII-8 with one character per byte, according to ISO 8859-1.

8.3.3 Mapping of data elements into constructed templates

Data elements are grouped into templates, which are located in Elementary Files (EF). If a record structured EF is used for storing data elements, one or more data elements are mapped onto the value field of a record coded in simple TLV.

The following constructed templates are described :

- Template h'61' Application template
- Template h'65' Cardholder related data
- Template h'66' Card data
- Template h'67' Authentication data
- Template h'6E' Application related data
- Template h'70' Logging parameters
- Template h'71' Reference transaction parameters
- Template h'72' Updatable transaction parameters
- Template h'73' Log data

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

8.3.3.1 Application template (Tag '61')

According to ISO/IEC 7816-5, clause 5, the only mandatory object is : Application identifier (AID) (#321) Tag h'4F'

. Application label (#304) Tag h'50'

8.3.3.2 Cardholder related data (Tag '65')

This template contains :

. Cardholder name (#202) Tag h'5F20'
. Cardholder name extended (#203) Tag h'80'
. Language preferences (#204) Tag h'5F2D'
. Address (#213) : Tag h'5F42'
. Date of birth (#214) : Tag h'5F2B'
. Special user requirements (#215): Tag h'68'

8.3.3.3 Card data (Tag '66')

This template contains the data elements which indicate operating characteristics of the card.

The following data elements should be present either in the historical bytes of the Answer To Reset or within the ATR file with the tags : h'5x', h'6x' or h'7x' :

* h'45' (in ATR file) : Card Issuer's data (see ISO/IEC 7816-4 subclause 8.3.4)

- Embedder/IC assembler Identifier (#103)

* h'67' (in ATR) : Pre-issuing data (see ISO/IEC 7816-4 subclause 8.3.5)

- IC manufacturer (#101)
- manufacturer's IC type identifier (#102)

- IC serial number (#105)

* h'71' or h'72' (if ATR) or h'47' (if ATR file) card capabilities (see ISO/IEC 7816-4 subclause 8.3.6)

- the First Software Function Table in which the card logical structure is indicated by the value :

- if = b'00000xxx' :MF only card
- if not = b'00000xxx' : MF-DF card

- the Second Software Function Table, which contains the data coding byte.

- the Third Software Function Table.

and :

. Card personaliser identifier (#201) tag h'80'
. CDF activator identifier (#206) tag h'81'
. CDF activator serial number (#207) tag h'82'
. Card effective date (#208) Tag h'5F26'
. Card expiry date (#217) Tag h'59'
. Card sequence number (#307) Tag h'5F34'
. Country code (#308) Tag h'5F28'

8.3.3.4 Authentication data (Tag '67')

This template contains :

. Key identifier (#107) Tag h'80'
. Authentication algorithm identifier (#601) Tag h'81'
. Derivation parameter(s) (#602) Tag h'82'
. Derivation function identifier (#603) Tag h'83'
. External authentication related data (#607) tag h'84'
. one-step/key number (#608) Tag h'85'
. one-step/signed data (#609) Tag h'86'
. two-step/trusted third party key number (#610) Tag h'87'
. two-step/signed data #1 (#611) Tag h'88'
. two-step/public exponent #2 (#612) Tag h'89'
. two-step/signed data #2 (#613) Tag h'8A'

8.3.3.5 Digital signature data (Tag '69')

This template contains data element tags selected by the issuer to be used by digital signature.

8.3.3.6 Application related data (Tag '6E')

This template contains :

. Track 1 (#209) Tag h'56'
. Track 2 (#210) Tag h'57'
. Track 3 (#211) Tag h'58'
. Cardholder identification number (#305) Tag h'5A'
. Application effective date (#309) Tag h'5F25'
. Application expiry date (#310) Tag h'5F24'
. Service code (#315) Tag h'5F30'
. Currency code (#316) Tag h'5F2A'
. Currency exponent (#317) Tag h'5F36'
. Application interchange profile (#322) Tag h'80'
. Application data list (#323) Tag h'81'

8.3.3.7 Logging parameters (Tag '70')

This template contains :

. Transaction log indicator (#501) Tag h'81'
. File-id for logging (#502) Tag h'82'
. Data elements for logging (#503) Tag h'83'

8.3.3.8 Reference transaction parameters (Tag '71')

This template contains :

. Floor limit (#401) Tag h'80'
. Maximum number of off-line authorisations (#402) Tag h'81'
. Maximum consecutive days off-line (#404) Tag h'82'
. Maximum total off-line amount (#406) Tag h'83'
. Revolving credit limit (#408) Tag h'84'
. Revolving credit cycle length (#409) Tag h'85'

8.3.3.9 Updatable transaction parameters (Tag '72')

This template contains :

. Number of consecutively performed off-line authorisations (#403) Tag h'80'
. Date latest on-line authorisation (#405) Tag h'81'
. Total off-line amount (#407) Tag h'82'
. Revolving credit cycle begin (#410) Tag h'83'
. Amount remaining this cycle (#411) Tag h'84'
. Remaining credit (#412) Tag h'85'
. Cash/Debit Account Amount remaining (#413) Tag h'86'

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

. Transaction authorising capability indicator (#414) Tag h'87'

8.3.3.10 Log data (Tag '73')

The content of the record depends on the value of the data element #503 among the following :

. Application Transaction counter (#415) Tag h'5F32'
. Transaction date (#504) Tag h'80'
. Transaction time (#505) Tag h'81'
. Card acceptor name and location (#506) Tag h'82'
. Transaction certificate (#418) Tag h'83'
. Processing code (#509) Tag h'84'
. Transaction amount (file currency) (#510) Tag h'85'
. Transaction amount (original currency) (#511) Tag h'86'
. Original currency code (#512) Tag h'87'
. Transaction Authorising source (#513) Tag h'88'
. Authorisation code (#514) Tag h'89'

8.3.4 Tables of constructed templates

These tables are contained in Annex A.

8.3.5 Division of large templates

When a template contains data elements whose total length exceeds 256 bytes, the data elements may be divided into more than one template having the same tag.

8.4 Mapping of constructed templates into Elementary Files

An Elementary File is a set of one or more constructed templates as defined in subclause 8.2.

The following Elementary Files are defined :

- ATR_EF, optional ;
- DIR_EF, optional ;
- COP_EF, optional ;
- REF_EF, optional ;
- UPD_EF, optional ;
- LOG_EF, optional.

8.4.1 ATR_EF

This EF is located under the MF, public read, no write, EF-ID = h'2F01'.

See contents in subclause 8.3.3.3 of this International Standard.

8.4.2 DIR_EF

This EF is located under the MF, public read, no write, EF-ID = h'2F00'.

See contents in subclause 8.3.3.1 of this International Standard.

8.4.3 COP_EF

This EF is located under the MF or a DF, read only, no write, EF-ID = h'2F10', file structure linear variable or linear fixed.

It may contain constructed templates '65', '66', '67' and '6E'.

8.4.4 REF_EF

This EF is located under the MF or DF, public read, no write, EF-ID = h'2F11', file structure linear variable or linear fixed.

It contains constructed templates '70' and '71'.

8.4.5 UPD_EF

This EF is located under the MF or DF, public read, updatable, EF-ID = h'2F12', file structure linear variable or linear fixed.

It contains constructed template '72'.

8.4.6 LOG_EF

This EF is located under the MF or DF, public read, updatable, file structure cyclic. The EF-ID is retrieved from (#502) File ID for logging.

It contains constructed template '73'.

8.5 Types of ICC logical structures

8.5.1 Structure of EFs

If present, a COP_EF shall be located at least at the MF level ; optionally, COP_EFs may additionally be located at DF level. If present, the optional ATR_EF and DIR_EF shall be located at MF level.

The other EFs, which are all optional, may be located either at the MF level or under a DF.

The short EF-ID of those optional EFs which are located under the MF shall be coded according to 8.4

EFs are of linear fixed or linear variable structure, except for log files which are of cyclic structure. Therefore, the file descriptor byte of EFs is as follows :

- h'02' = linear fixed, no further info
- h'03' = linear fixed, TLV coded
- h'05' = linear variable, TLV coded
- h'06' = cyclic, no further info
- h'07' = cyclic, TLV coded.

Elementary Files structures features are described in the card capabilities data elements of the historical bytes. See subclause 4.9.

The coding of the security attributes is application dependent and is not specified in this International Standard.

8.5.2 Structure of files

The logical structure of ICC may be either MF only or MF and one or more DF(s).

The absence of DF(s) in an ICC is indicated by the value b'00000xxx' of the First Software Function Table of the historical bytes (if present).

The specific data described in this standard are located in EFs the file ID of which is h'2F1x' when at master file level.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

8.5.3 Example of logical structure of the EFs

Some examples of logical structure are shown in Annex B and are explained here below.

The logical structure of an ICC is composed of a CDF and optionally of ADF(s) as defined in ISO 9992-1.

Financial interchange is achieved using data elements contained in elementary files present in the CDF and/or ADF(s).

Depending on the capabilities of the ICCs and the choice of the issuer, the data relates to the following types of logical structures :

- the CDF of a MF only card.
- the CDF and/or the ADF in a card with a MF and one DF for interchange.
- the CDF and the ADF chosen from the set of available DFs in a card with a MF and several DFs for interchange.

Those data elements not present in the ADF and required to perform the transaction shall be taken from the CDF.

In a financial transaction card, the CDF is located at the MF level (file-ID = h'3F00') ; when present, any ADF shall be located at DF level.

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

Annex A
(normative)

Contents of constructed templates

Legend : Element # refers to the numbering of clause 8.
M means mandatory.
O means optional.
Min is Minimum length in bytes.
Max is Maximum length in bytes.

Template h'61' : Application template

Tag	#	M/O	Name	Length	Format	Min M	Min M+O	Max
4F	321	M	Application Identifier	5-16	b	5	5	16
50	304	O	Application label	-12	an			12

Template h'65' : Cardholder related data

Tag	#	M/O	Name	Length	Format	Min M	Min M+O	Max
5F20	202	O	Cardholder name	2-26	an		3	27
5F2B	214	O	Date of birth	8	n		4	4
5F2D	204	O	Language preferences	2-8	a		3	9
5F42	213	O	Address	-192	ans		0	192
68	215	O	Special user requirements	-10	b		1	10
80	203	O	Cardholder name extended	26	an		26	26

Template h'66' : Card data

Tag	#	M/O	Name	Length	Format	Min M	Min M+O	Max
45	103	M	Embedder/IC assembler Identifier	5	an	5	5	5
46	101	M	IC manufacturer identifier	1	b	1	1	1
	102	M	Manufacturer's IC type identifier	2	b	2	2	2
	105	O	IC serial number	4	b		4	4
59	217	M	Card expiry date	4	n	2	2	2
5F26	208	O	Card effective date	6	n		3	3
5F28	308	O	Country code	3	n		2	2
5F34	307	O	Card sequence number	3	n		2	2
80	201	O	Card personaliser identifier	1	b		1	1
81	206	O	CDF activator identifier	4	n		2	2
82	207	O	CDF activator serial number	6	n		3	3

Template h'67' : Card authentication data

Tag	#	M/O	Name	Length	Format	Min M	Min M+O	Max
5F29	212	M	Card Interchange profile	2-3	b	2	2	3
80	107	O	Key identifier	1	b		1	1
81	601	O	Authentication algorithm identifier	1	b	1		1
82	602	O	Derivation parameter(s)	?	b	?		?
83	603	O	Derivation function identifier	1	b	1		1
84	607	O	External authentication related data	-8	b		2	8
85	608	O	One step/key number	-21	b			21
86	609	O	One step/signed data	-128	b		40	128
87	610	O	Two step/trusted third party key number	-21	b			21
88	611	O	Two step/signed data # 1	128	b		40	128
89	612	O	Two step/public exponent # 2	1	b		1	1
8A	613	O	Two step/signed data # 2	-128	b		40	128

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998

Template h'69' : Digital signature data

At the issuer's discretion.

Template h'6E' : Application Related data

Tag	#	M/O	Name	Length	Format	Min M	Min M+O	Max
56	209	O	Track 1	13-76	ans		14	77
57	210	O	Track 2	9-37	ans		10	38
58	211	O	Track 3	-104	ns			104
5A	305	M	Cardholder identification number	19	n	10	10	10
5F24	310	O	Application expiry date	4	n		2	2
5F25	309	O	Application effective date	6	n		3	3
5F2A	316	O	Currency code	3	n		2	2
5F30	315	M	Service code	3	n	2	2	2
5F36	317	O	Currency exponent	1	n		1	1
80	322	O	Application interchange profile	2-3	b	2	2	3
81	323	O	Application data list	-128	b			128

Template h'70' : Logging parameters

Tag	#	M/O	Name	Length	Format	Min M+O	Max
81	501	O	Transaction log indicator	1	n	1	1
82	502	O	File-id for logging	2	b	1	1
83	503	O	Data elements for logging.	n*2	b	2	2

Template h'71' : Reference transaction parameters

Tag	#	M/O	Name	Length	Format	Min M+O	Max
80	401	O	Floor limit	7	n	4	4
81	402	O	Maximum number of off-line authorisations	2	n	1	1
82	404	O	Maximum consecutive days off-line	3	n	2	2
83	406	O	Maximum total off-line amount	8	n	4	4
84	408	O	Revolving credit limit	8	n	4	4
85	409	O	Revolving credit cycle length	2	n	1	1

Template h'72' : Updatable transaction parameters

Tag	#	M/O	Name	Length	Format	Min M+O	Max
80	403	O	Number of consecutively performed off-line authorisations	2	n	1	1
81	405	O	Date latest on-line authorisation	6	n	3	3
82	407	O	Total off-line amount	8	n	4	4
83	410	O	Revolving credit cycle begin	5	n	3	3
84	411	O	Amount remaining this cycle	8	n	4	4
85	412	O	Remaining credit	8	n	4	4
86	413	O	Cash/Debit Account Amount remaining	12	n	6	6
87	414	O	Transaction Authorising capability Indicator	1	b	1	1

STANDARDSISO.COM : Click to view the full PDF of ISO 9992-2:1998