IS 15043 (Part 1) : 2001
ISO 9992-1 : 1990

भारतीय मानक

वित्तीय लेन देन कार्ड — एकीकृत परिपथ कार्ड एवं कार्ड स्वीकरण यंत्र के बीच संदेश

भाग 1 संकल्पनाऐं एवं संरचना

Indian Standard

FINANCIAL TRANSACTION CARDS — MESSAGES BETWEEN THE INTEGRATED CIRCUIT CARD AND THE CARD ACCEPTING DEVICE

PART 1 CONCEPTS AND STRUCTURES

ICS 35.240.15

BUREAU OF INDIAN STANDARDS
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

December 2001

Price Group 3

NATIONAL FOREWORD

This Indian Standard (Part 1) which is identical with ISO 9992-1 : 1990 'Financial transaction cards — Messages between the integrated circuit card and the card accepting device—Part 1: Concept and structures' issued by the International Organization for Standardization (ISO) was adopted by the Bureau of Indian Standards on the recommendation of the Banking and Financial Services Sectional Committee (MSD 7) and approval of the Management and Systems Division Council.

The text of the International Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

> Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

In the adopted standard, normative reference appears to certain International Standards for which Indian Standards also exist. The corresponding Indian Standards which are to be substituted in their place are listed below along with their degree of equivalence for the editions indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO 7810 : 1985	IS 14172 : 1994/ISO 7810 : 1985 Identification cards — Physical characteristics	Identical
ISO 7812 : 1987	IS 14173 : 1994/ISO 7812 : 1987 Identification cards — Numbering system and registration procedure for issues identifier	do
ISO 7813 : 1990	IS 14174 : 1994/ISO 7813 : 1990 Identification cards — Financial transaction cards	do
ISO 10202	IS 14958 (Part 1) : 2001/ISO 10202-1 : 1991 Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards: Part 1 Card life cycle	do
	IS 14958 (Part 2) : 2001/ISO 10202-2 : 1996 Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards: Part 2 Transaction process	do
	IS 14958 (Part 3) : 2001/ISO 10202-3 : 1998 Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards: Part 3 Cryptographic key relationships	do
	IS 14958 (Part 4) : 2001/ISO 10202-4 : 1996 Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards: Part 4 Secure application modules	do
	IS 14958 (Part 5) : 2001/ISO 10202-5 : 1998 Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards: Part 5 Use of algorithms	do
	IS 14958 (Part 6) : 2001/ISO 10202-6 : 1994 Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards: Part 6 Cardholder verification	do
	IS 14958 (Part 7) : 2001/ISO 10202-7 : 1998 Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards: Part 7 Key management	do
	IS 14958 (Part 8) : 2001/ISO 10202-8 : 1998 Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards: Part 8 General principles and overview	do

(*Continued on third cover*)

Indian Standard

FINANCIAL TRANSACTION CARDS — MESSAGES BETWEEN THE INTEGRATED CIRCUIT CARD AND THE CARD ACCEPTING DEVICE

PART 1 CONCEPTS AND STRUCTURES

Introduction

The concepts on which this part of ISO 9992 has been developed are based upon the following considerations :

- this part of ISO 9992 provides compatibility with existing ISO standards referenced in clause 2 and is intended to provide the flexibility to accommodate future Integrated Circuit Card (ICC) technology;

- this part of ISO 9992 supports the use of a single application or multiple applications in an ICC. When more than one application exists in the ICC, multiple applications of the same type of service (e.g. electronic chequebook) may be present. Applications may be added to the ICC at any time during its life cycle, with the agreement of the issuer, and according to security rules defined in ISO 10202. An application may be logically deleted from the ICC at any time during its life cycle, in accordance with agreed procedures between the operating parties.

1 Scope

This part of ISO 9992 is applicable to the use of Integrated Circuit Cards issued by Financial Institutions in retail financial applications in an interchange environment. It specifically addresses :

- the functions required for financial interchange,

- the structure and types of messages between the Integrated Circuit Card (ICC) and the Card Accepting Device (CAD) to effect those functions,

- the identification and definition of data elements which may or shall be used during exchanges between the ICC and the CAD.

ISO 9992-1 establishes the concepts by which the ICC and the CAD exchange messages. This makes it necessary also to describe the logical structure of data within the ICC.

This part of ISO 9992 defines messages to support the security requirements of authentication (e.g. card authentication, CAD authentication, cardholder verification). It does not specify or recommend any method or procedure. Security techniques shall be implemented in accordance with ISO 10202.

This part of ISO 9992 is independent of the capabilities of the CAD (connectable or not, attended or unattended) and its status (on-line or off-line).

This part of ISO 9992 does not define the methodologies deployed to implement an application.

This part of ISO 9992 is based on the existence of a logical data structure and provides rules for the way data in the ICC is logically referenced by the CAD. It does not define how data is physically structured in the ICC.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 9992. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 9992 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

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

ISO 7810 : 1985, *Identification cards - Physical characteristics.*

ISO 7812 : 1987, *Identification cards - Numbering system and registration procedure for issuer identifiers*

ISO 7813 : 1987, *Identification cards - Financial transaction cards.*

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

ISO 7816-4 : ---- [1], *Identification cards - Integrated circuit(s) cards with contacts. Part 4 : Interindustry commands (under study by ISO /IEC 1 /17/4)*

ISO 10202 : -----[1], *Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards.* [1]

---

1) **To be published.**

3 Definitions and abbreviations

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 Card.

command: A request or advice message which initiates an action and which solicits a response.

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

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

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

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

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

Primary Account Number (PAN): The assigned number that identifies the card issuer and cardholder. This number is composed of an issuer identification number, individual account identification, and an accompanying check digit.

NOTE: Equivalent to identification number, as specified in ISO 7812. See also ISO 4909.

Personal Identification Number (PIN): The code or password the customer possesses for verification of identity.

response: A message returned to the initiator after the processing of a command to the recipient.

4 Concepts and structures

4.1 Logical structure of the data within the ICC

The logical data structure enables an ICC to support, with the minimum duplication of data, services independent from each other. These services may be provided by different application suppliers.

Data that may be used by all services supported by an ICC (e.g. PAN, card expiry date) are contained in the Common Data File (CDF). Only one CDF shall be present in an ICC. The card issuer shall be responsible for the presence, contents and use of the CDF.

Data stored in an ICC to service a business transaction is contained in the CDF and/or in an Application Data File (ADF). One or more ADF may be present in an ICC to accommodate different financial and non-financial services.

An ICC may contain a CDF without the presence of an ADF.

4.2 Interactions between the ICC and the CAD

The ICC and the CAD interact using messages. These messages, which are commands and their responses, are used to accomplish functions which are part or all of a transaction.

Annex A illustrates the relationships which are described hereafter.

4.2.1 Relationship between transactions and functions

A transaction (e.g. cash withdrawals, purchase, PIN change) consists of one or more functions (e.g. cardholder verification, CAD authentication, transaction recording).

Those functions which are defined as either mandatory or recommended for use in international financial interchange are specified in part 2 of this International Standard. Additional functions may be added to support activities defined by bilateral agreements.

4.2.2 Relationship between functions and messages

A function as described in 4.3.1 shall be accomplished using one or more pairs of messages. These messages are commands (e.g. read, write) and their responses (e.g. acknowledgement, data). After processing a command, resulting in a decision and/or an action, the receiver shall return a response to the sender.

The commands and responses used to accomplish each function are identified in part 3 of this International Standard.

Generic commands are described in ISO 7816-4. Financial ICC specific commands are described in part 3 of this International Standard.

4.3 Data access attributes

4.3.1 Read access attributes

Three classes of read access are defined :

- Public Read Access (PR): The data is available to the CAD without any restriction;

- Conditional Read Access (CR): The data is available only after specific criteria have been met;

- No Read Access (NR): The data shall never be read by the CAD.

4.3.2 Write access attributes

Three classes of write access are defined :

- Free Write Access (FW): The data may be added, modified or deleted without any restriction;

- Conditional Write Access (CW) : The data may be added, modified or deleted only after specific criteria have been met;

- One time Write Access (OW) : The data, once written, cannot be altered or modified.

4.4 Compatibility with present technology

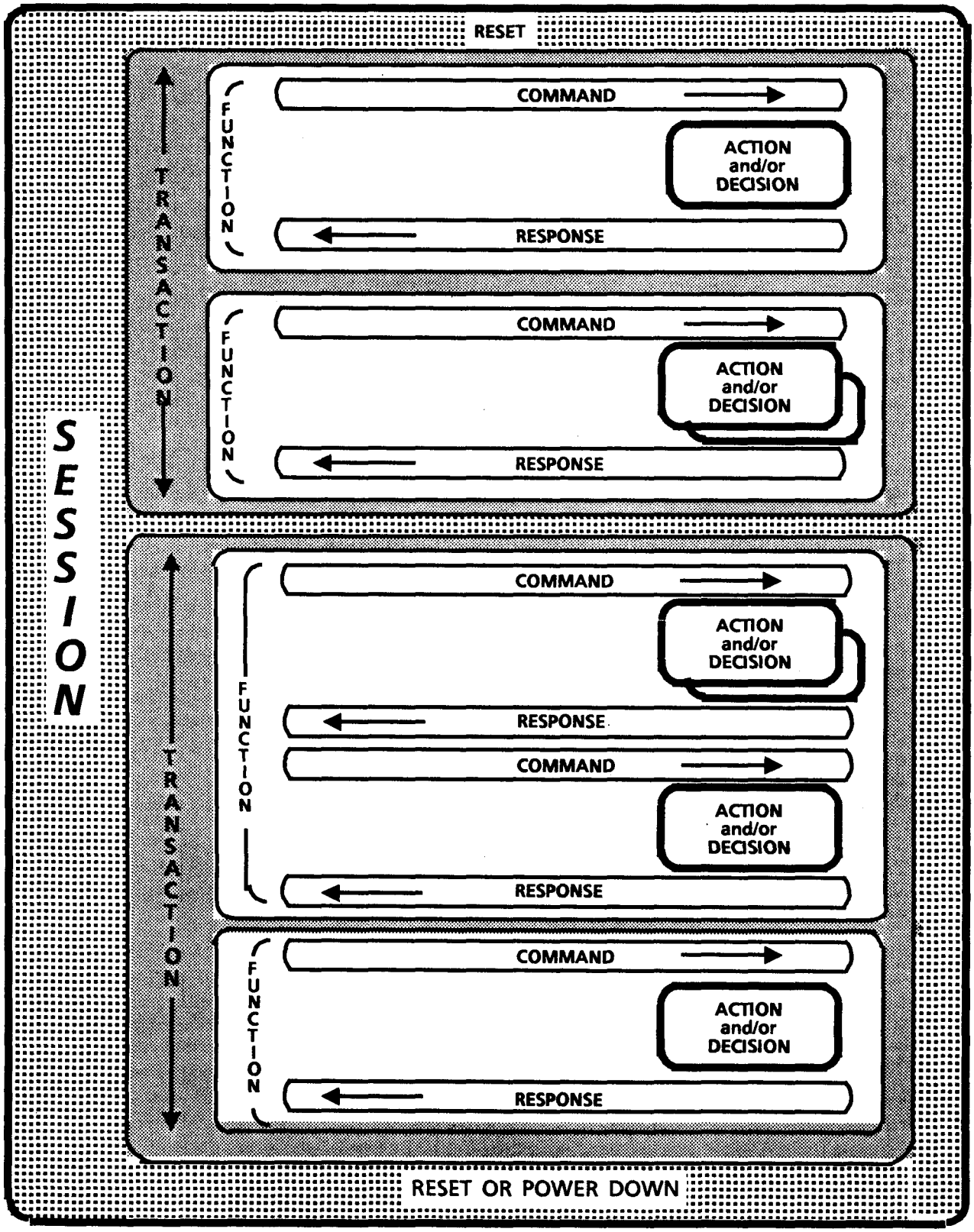
The Primary Account Number, or PAN, shall always be present in the CDF (see ISO 7812, 7813 and 4909).

If the ICC also contains an embossed PAN and/or magnetic stripes encoded according to ISO 7813, the International Interchange PAN in the CDF shall be identical to that embossed and/or that encoded in the magnetic stripes.

Annex A

(informative)

Relationships between transactions, functions and messages



Notations on ICC relationships

The schematic shows the relationships between the components of a session initiated by the insertion of an ICC into the CAD and terminated by its removal.

The illustration is not intended to show that the flow is unidirectional (from CAD to ICC), nor does it imply that future technology will be restricted to these boundaries (e.g. an entire transaction may be accomplished by a single command and response).

Three levels of relationships are identified in this schematic.

a) function consisting of a single command which causes a single action or decision followed by a response is expressed as

$$F = [C1 + A1/D1 + R1]$$

b) function consisting of multiple sets of commands, actions/decisions and responses is expressed as

$$F = [(C1 + A1 + R1) + (C2 + D2 + R2)... + (C5 + D5 + R5)]$$

c) function consisting of a single command and response that has multiple actions and decisions is expressed as

$$F = [C1 + (A1 + D2 + A3) + R1]$$

where F is the function

C1, C2 etc. are commands;
A1, A2 etc. are actions;
D1, D2 etc. are decisions; and
R1, R2 etc. are responses.

(*Continued from second cover*)

The International Standard ISO 7812 for which the corresponding Indian Standard is IS 14173 : 1994/ ISO 7812 : 1987 has since been revised and has been published in the following two parts:

ISO/IEC 7812-1 : 1993	Identification cards — Identification of issuers: Part 1 Numbering system
ISO/IEC 7812-2 : 1993	Identification cards — Identification of issuers: Part 2 Application and registration procedures

The International Standard ISO 7813 for which the corresponding Indian Standard is IS 14174 : 1994/ ISO 7813 : 1990 has since been revised as the following standard:

ISO/IEC 7813 : 1995	Identification cards — Financial transaction cards

In the adopted standard, normative references also appear to the following International Standards for which no Indian Standards exist:

ISO 4909 : 1987	Bank cards — Magnetic stripe data content for track 3
ISO/IEC 7816-3 : 1989	Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols
ISO/IEC 7816-4	Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange

The technical committee responsible for the preparation of this standard has reviewed the provisions of the above referred standards and has decided that they are acceptable for use in conjunction with this standard.

The International Standard ISO 4909 has been revised and the details of revised version are given below:

ISO 4909 : 2000	Bank cards — Magnetic stripe data content for track 3

The revised version is under consideration for adoption as an Indian Standard.

So far, two parts of the International Standard ISO 9992 have been published. The following part of this International Standard is under consideration for adoption as an Indian Standard:

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

Annex A of this standard is for information only.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act,* 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc : No. MSD 7 (181).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters :

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110 002
Telephones : 323 01 31, 323 33 75, 323 94 02

Telegrams : Manaksanstha
(Common to all offices)

Regional Offices :		Telephone
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110 002	323 76 17 323 38 41
Eastern	: 1/14 C.I.T. Scheme VII M, V. I. P. Road, Kankurgachi KOLKATA 700 054	337 84 99, 337 85 61 337 86 26, 337 91 20
Northern	: SCO 335-336, Sector 34-A, CHANDIGARH 160 022	60 38 43 60 20 25
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600 113	254 12 16, 254 14 42 254 25 19, 254 13 15
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400 093	832 92 95, 832 78 58 832 78 91, 832 78 92

Branches : AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. NAGPUR. NALAGARH. PATNA. PUNE. RAJKOT. THIRUVANANTHAPURAM.

Printed at Prabhat Offset Press, New Delhi-2