IS 15042 (Part 1) : 2001
ISO 9564-1 : 1991

भारतीय मानक

बैंकिंग — व्यक्तिगत पहचान नम्बर प्रबंधन एवं सुरक्षा

भाग 1 पिन रक्षण सिद्धान्त एवं तकनीक

Indian Standard

BANKING — PERSONAL IDENTIFICATION NUMBER MANAGEMENT AND SECURITY

PART 1 PIN PROTECTION PRINCIPLES AND TECHNIQUES

ICS 35.240.40

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

November 2001

Price Group 10

NATIONAL FOREWORD

This Indian Standard (Part 1) which is identical with ISO 9564-1:1991 'Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques' 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 the following International Standard for which Indian Standard also exists. The corresponding Indian Standard which is to be substituted in its place is listed below along with its degree of equivalence for the edition indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO 7812 : 1987	IS 14173 : 1994/ISO 7812:1987 Identification cards — Numbering system and registration procedure for issuer identifier	Identical

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

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

ISO 8583 : 1987	Bank card originated messages — Interchange message specifications — Content for financial transactions
ISO 8908 : 1993	Banking and related financial services — Vocabulary and data elements
ISO 9807 : 1991	Banking and related financial services — Requirements for message authentication (retail)
ANSI X3.92 : 1981	Data Encryption Algorithm (DEA)

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.

(*Continued on third cover*)

Contents

Page

1 Scope 1

2 Normative references 1

3 Definitions 2

4 Basic principles of PIN management 3

5 PIN pads 4

5.1 Character set 4

5.2 Character representation 4

5.3 PIN entry 4

5.4 Packaging considerations 4

6 PIN security issues 5

6.1 PIN control procedures 5

6.2 PIN encipherment 5

6.3 Physical security 6

7 Techniques for management/protection of account-related PIN functions 7

7.1 PIN length 7

7.2 PIN selection 7

7.3 PIN delivery and issuance 8

7.4 PIN change 9

7.5 Disposal of waste material and returned PIN mailers 9

7.6 PIN activation 10

7.7 PIN storage 10

7.8 PIN deactivation 10

8 Techniques for management/protection of transaction-related PIN functions 10

8.1 PIN entry 10

8.2 Protection of PIN during transmission 10

8.3 Standard PIN block formats 11

8.4 Other PIN block formats 12

8.5 PIN verification 12

8.6 Journaling of transactions containing PIN data 12

9 Approval procedure for encipherment algorithms 13

Annexes

A Procedure for approval of an encipherment algorithm 14

B General principles of key management 16

C PIN verification techniques 18

D PIN entry device 19

E Example of pseudo-random PIN generation 21

F Additional guidelines for PIN pad design 22

G Guidance on clearing and destruction procedures for sensitive data 25

H Information for customers 28

Introduction

The Personal Identification Number (PIN) is a means of verifying the identity of a customer within an electronic funds transfer (EFT) system.

The objective of PIN management is to protect the PIN against unauthorized disclosure, compromise, and misuse throughout its life cycle and in so doing to minimize the risk of fraud occurring within EFT systems. The secrecy of the PIN needs to be assured at all times during its life cycle which consists of its selection, issuance, activation, storage, entry, transmission, validation, deactivation, and any other use made of it.

PIN security also depends upon sound key management. Maintaining the secrecy of cryptographic keys is of the utmost importance because the compromise of any key allows the compromise of any PIN ever enciphered under it.

Wherever possible, this part of ISO 9564 specifies requirements in absolute terms. In some instances a level of subjectivity cannot be practically avoided especially when discussing the degree of level of security desired or to be achieved.

The level of security to be achieved needs to be related to a number of factors, including the sensitivity of the data concerned and the likelihood that the data will be intercepted, the practicality of any envisaged encipherment process, and the cost of providing, and breaking, a particular means of providing security. It is, therefore, necessary for each card Acceptor, Acquirer and Issuer to agree on the extent and detail of security and PIN management procedures. Absolute security is not practically achievable; therefore, PIN management procedures should implement preventive measures to reduce the opportunity for a breach in security and aim for a "high" probability of detection of any illicit access or change to PIN material should these preventive measures fail. This applies at all stages of the generation, exchange and use of a PIN, including those processes that occur in cryptographic equipment and those related to communication of PINs.

This part of ISO 9564 is designed so that Issuers can uniformly make certain, to whatever degree is practical, that a PIN, while under the control of other institutions, is properly managed. Techniques are given for protecting the PIN-based customer authentication process by safeguarding the PIN against unauthorized disclosure during the PIN's life cycle.

This part of ISO 9564 indicates techniques for protecting the PIN against unauthorized disclosure during its life cycle and includes the following annexes:

a) annex A gives the procedure for the approval of an encipherment algorithm;

b) annex B covers general principles of key management;

c) annex C covers techniques for PIN verification;

d) annex D deals with implementation concepts for a PIN entry device;

e) annex E identifies an example of pseudo-random PIN generation;

f) annex F indicates additional guidelines for PIN pad design;

g) annex G specifies the erasing of recording media used for storage of keying material;

h) annex H gives information for customers.

In ISO 9564-2, approved encipherment algorithms to be used in the protection of the PIN are specified. Application of the requirements of this part of ISO 9564 requires bilateral agreements to be made, including the choice of algorithms specified in ISO 9564-2.

This part of ISO 9564 is one of a series that describes requirements for security in the retail banking environment, as follows:

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

ISO 9564-2:1991, *Banking — Personal Identification Number management and security — Part 2: Approved algorithm(s) for PIN encipherment.*

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail).*

The requirements of ISO 9564 are compatible with those in ISO 8583 for the accommodation of security related data.

Indian Standard

BANKING — PERSONAL IDENTIFICATION NUMBER MANAGEMENT AND SECURITY

PART 1 PIN PROTECTION PRINCIPLES AND TECHNIQUES

1 Scope

This part of ISO 9564 specifies the minimum security measures required for effective international PIN management. A standard means of interchanging PIN data is provided. This part of ISO 9564 also specifies the rules related to the approval of PIN encipherment algorithms. This part of ISO 9564 is applicable to institutions responsible for implementing techniques for the management and protection of the PIN for bank card originated transactions. The provisions of this part of ISO 9564 are not intended to cover

— the protection of the PIN against loss or intentional misuse by the customer or authorized employees of the issuer;

— privacy of non-PIN transaction data;

— protection of transaction messages against alteration or substitution, e.g. an authorization response to a PIN verification;

— protection against replay of the PIN or transaction;

— specific key management techniques;

— PIN management and security for transactions conducted using Integrated Circuit Cards (ICC);

— the use of asymmetric encipherment algorithms for PIN management.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 9564. 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 9564 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 7812:1987, *Identification cards — Numbering system and registration procedure for issuer identifiers.*

ISO 8583:1987, *Bank card originated messages — Interchange message specifications — Content for financial transactions.*

ISO 8908:—[1], *Banking and related financial services — Vocabulary and data elements.*

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail).*

American National Standard X3.92:1981, *Data Encryption Algorithm (DEA).*

3 Definitions

For the purposes of this part of ISO 9564, the following definitions apply.

3.1 acquirer: The institution (or its agent) which acquires from the card acceptor the financial data relating to the transaction and initiates that data into an interchange system.

3.2 algorithm: A clearly specified mathematical process for computation.

3.3 card acceptor: The party accepting the card and presenting transaction data to an acquirer.

3.4 cipher text: Data in its enciphered form.

3.5 compromise: In cryptography, the breaching of secrecy and/or security.

3.6 cryptographic key: A mathematical value which is used in an algorithm to transform plain text into cipher text or vice versa.

3.7 customer: The individual associated with the primary account number (PAN) specified in the transaction.

3.8 decipherment: The reversal of a previous reversible encipherment, rendering cipher text intelligible.

3.9 dual control: A process of utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single entity is able to access or utilize the materials, e.g. cryptographic key.

3.10 encipherment: The rendering of text unintelligible by means of an encoding mechanism.

3.11 irreversible encipherment: Transformation of plain text to cipher text in such a way that the original plain text cannot be recovered by other than exhaustive procedures even if the cryptographic key is known.

3.12 irreversible transformation of a key: Generation of a new key from the previous key such that there is no feasible technique for determining the previous key given a knowledge of the new key and of all details of the transformation.

3.13 issuer: The institution holding the account identified by the primary account number (PAN).

3.14 key component: One of at least two parameters having the format of a cryptographic key that is added modulo-2 with one or more like parameters to form a cryptographic key.

3.15 modulo-2 addition: Binary addition with no carry (also called Exclusive OR'ing).

3.16 node: Any message processing entity through which a transaction passes.

3.17 notarization: A method of modifying a key enciphering key in order to authenticate the identities of the originator and the ultimate recipient.

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

3.19 plain text: Data in its original unenciphered form.

---

1) To be published.

3.20 primary account number (PAN): The assigned number that identifies the card issuer and card holder. This number is composed of an issuer identification number, an individual account identification, and an accompanying check digit, as defined in ISO 7812.

3.21 pseudo-random number: A number that is statistically random and essentially unpredictable although generated by an algorithmic process.

3.22 reference PIN: The value of the PIN used to verify the transaction PIN.

3.23 reversible encipherment: Transformation of plain text to cipher text in such a way that the original plain text can be recovered.

3.24 split knowledge: A condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key.

3.25 transaction PIN: The term used to describe the PIN as entered by the customer.

3.26 variant of a key: A new key formed by a non-secret process with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.

4 Basic principles of PIN management

PIN management shall be governed by the following basic principles.

a) For all PIN management functions, controls shall be applied so that hardware and software used cannot be fraudulently modified or accessed without recording, detection and/or disabling as defined in 6.1.1.

b) After selection the PIN, if stored, shall be enciphered when it cannot be physically secured as defined in 6.2 and 7.7.

c) For different accounts, encipherment of the same PIN value under a given encipherment key shall not predictably produce the same cipher text as defined in 6.2.

d) Security of an enciphered PIN shall not rely on the secrecy of the encipherment design or algorithm but on a secret key as defined in 6.2.

e) The plain text PIN shall never exist in the facility of the acquirer except within a physically secure device as defined in 6.3.1.

f) A plain text PIN may exist in the general purpose computer facility of the issuer if the facility is a physically secure environment at the time as defined in 6.3.2.

g) Only the customer and/or personnel authorized by the issuer shall be involved with PIN selection (see 7.2), PIN issuance, or any PIN entry process in which the PIN can be related to account identity information. Such personnel shall operate only under strictly enforced procedures (e.g. under dual control).

h) A stored enciphered PIN shall be protected from substitution as defined in 7.7.

i) Compromise of the PIN (or suspected compromise) shall result in the ending of the PIN life cycle as defined in 7.8.

j) Responsibility for PIN verification shall rest with the issuer although the verification function may be delegated to another institution as defined in 8.5.

k) Different encipherment keys shall be used for protection of PIN storage and transmission as defined in 6.2.

l) The customer shall be advised in writing of the importance of the PIN and PIN secrecy (see annex H).

5 PIN pads

5.1 Character set

All PIN pads shall provide for the entry of the decimal numeric characters 0 (zero) to 9 (nine).

NOTE 1 It is recognized that alphabetic characters, although not assigned in this part of ISO 9564, may be used as synonyms for decimal numeric characters. Further guidance on the design of PIN pads, including alpha to numeric mappings, is given in annex F.

5.2 Character representation

The relationship between the numeric value of a PIN character and the internal coding of that value prior to any encipherment shall be as specified in table 1.

Table 1 — Character representation

PIN character	Internal binary
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

5.3 PIN entry

The values of the entered PIN shall not be displayed in plain text or be disclosed by audible feedback.

5.4 Packaging considerations

A PIN pad may be packaged as an integral part of the terminal, or may be remote from the terminal control electronics. The terminal control electronics may or may not be physically secure (see 6.3.1 for definition); however, the PIN pad shall be secured as specified in 6.3.1 or 6.3.3.

The PIN pad shall be designed or installed so that the customer can prevent others from observing the PIN value as if is being entered.

When a remote PIN pad is used the communications link between it and its associated terminal shall be protected (see 8.2).

Table 2 summarizes the security requirements for each of the four possible configurations of terminal and PIN pad.

Table 2 — PIN pad packaging considerations

	Terminal physically secure	Terminal physically insecure
PIN pad integral to terminal	Physical protection requirements as specified in 6.3.1 apply to the whole terminal. Terminal shall encipher PIN as specified in 6.2 for transmission.	Physical protection requirements as specified in 6.3.1 or 6.3.3 apply to PIN pad. PIN pad shall encipher PIN as specified in 6.2 for transmission.
PIN pad remote to terminal	The PIN pad shall be secured as specified in 6.3.1 or 6.3.3. PIN pad shall encipher PIN as specified in 6.2 for transmission.	The PIN pad shall be secured as specified in 6.3.1 or 6.3.3. PIN pad shall encipher PIN as specified in 6.2 for transmission.

6 PIN security issues

6.1 PIN control procedures

6.1.1 Hardware and software

Hardware and software used in PIN management functions shall be implemented in such a way that the following are assured.

a) The hardware and software is correctly performing its designed function and only its designed function.

b) The hardware and software cannot be modified or accessed without detection and/or disabling.

c) Information cannot be fraudulently accessed or modified without detection and rejection of the attempt.

d) The system shall not be capable of being used or misused to determine a PIN by exhaustive trial and error.

NOTE 2 Printed or microfilm listings of programs or dumps used in the selection, calculation, or encipherment of the PIN should be controlled during use, delivery, storage, and disposal.

6.1.2 Recording media

Any recording media (e.g. magnetic tape, disks) containing data from which a plain text PIN might be determined shall be degaussed, overwritten, or physically destroyed immediately after use. Only if all storage areas (including temporary storage) used in the above process can be specifically identified and degaussed or overwritten may a computer system be used for these processes (see annex G).

6.1.3 Oral communications

No procedure shall require or permit oral communication of the plain text PIN, either by telephone or in person. An institution shall never permit its employees to ask a customer to disclose the PIN or to recommend specific values.

6.1.4 Telephone keypads

Procedures of an institution shall not permit entry of the plain text PIN through a keypad of a telephone, unless the telephone device is designed and constructed to meet the requirements specified in 5.4 for PIN pads and 8.2 for PIN transmission.

6.2 PIN encipherment

When it is necessary to encipher a PIN for storage or transmission (see 6.3 and 8.2), this shall be accomplished using one of the approved algorithms specified in ISO 9564-2.

The adopted encipherment procedure shall ensure that the encipherment of a plain text PIN value using a particular cryptographic key does not predictably produce the same enciphered value when the same PIN value is associated with different accounts (see 7.8).

Different encipherment keys shall be used to protect the reference PIN and the transaction PIN.

PIN encipherment keys shall not be used for any other cryptographic purpose.

See annex B for general principles of key management.

6.3 Physical security

This subclause defines a "physically secure device" and a "physically secure environment", and specifies requirements for a PIN entry device.

An unenciphered reference PIN shall exist only within a "physically secure environment" or "physically secure device". An unenciphered transaction PIN shall exist only within a "physically secure device", a PIN entry device meeting the requirements of 6.3.3, or the issuer's (or issuer's agent's) "physically secure environment".

6.3.1 Physically secure device

In assessing the physical security of any device, the operating environment, in which the device is working, is an important consideration. A physically secure device is a hardware device which when operated in its intended manner and environment cannot be successfully penetrated to disclose all or part of any cryptographic key or PIN resident within the device.

Penetration of the device when operated in its intended manner and environment shall cause the automatic and immediate erasure of all PINs, cryptographic keys and all useful residue of PINs and keys contained within the device.

A device shall only be operated as a physically secure device when it can be assured that the device's internal operation has not been modified to allow penetration (e.g. the insertion within the device of an active or passive "tapping" mechanism).

6.3.2 Physically secure environment

A physically secure environment is one which is equipped with access controls or other mechanisms designed to prevent any penetration which would result in the disclosure of all or part of any cryptographic key or PIN stored within the environment.

A physically secure environment shall remain such until all PINs, cryptographic keys and useful residue from PIN and key have been erased from the environment.

6.3.3 PIN entry device requirements

A PIN entry device shall comply with the requirements of 6.3.1 or, at a minimum, meet the following requirements.

a) The transaction PIN shall be enciphered within the device in a manner allowed by clause 8.

b) Successful penetration of the PIN entry device shall not permit disclosure of any previously entered transaction PIN even with knowledge of additional relevant data which is, or has been, accessible external to the device (e.g. enciphered PINs as previously transmitted from the device).

c) The unauthorized determination of the secret data (PINs and keys) stored within the PIN entry device, or the placing within the device of a "tap" to record secret data, shall require that the device be taken to a specialized facility, and at this facility be subjected to physical damage such that the device cannot be placed back in service without a high probability of the tampering being detected. Furthermore, the deter-

mination of secret data or the placing of a "tap" within the device shall require specialized equipment and skills which are not generally available.

d) The data stored within a PIN entry device, even if determined, cannot be transferred into another such device.

NOTE 3 See annex D for guidance on implementation of a PIN entry device.

7 Techniques for management/protection of account-related PIN functions

7.1 PIN length

A PIN shall be not less than 4 and not more than 12 characters in length.

NOTE 4 While there is a security advantage to having a longer PIN, usefulness may be hindered. For usability reasons an assigned numeric PIN should not exceed 6 digits in length. It is recommended, for security reasons, that a customer selected alpha PIN should not be less than 6 characters in length. It should also be noted that many international systems do not accept more than 6 digits and/or do not support alpha PIN entry.

7.2 PIN selection

A PIN shall be selected using one or more of the following techniques:

— assigned derived PIN;

— assigned random PIN;

— customer selected PIN.

Compromise during PIN selection could prejudice the security of any issued PIN.

7.2.1 Assigned derived PIN

When the reference PIN is an "assigned derived PIN" the issuer shall derive it cryptographically from

a) the primary account number, and/or

b) some other value associated with the customer.

NOTES

5 The PIN derivation process should not contain a bias towards specific sets of values.

6 If this technique is used the issuer should not maintain any record of the PIN as the PIN can be derived as needed.

7 When the PIN is derived from card data, it may be used to validate that data.

7.2.2 Assigned random PIN

When the reference PIN is an "assigned random PIN" the issuer shall obtain a value by means of either

a) a true random number generator, or

b) a pseudo-random number generator (see annex E).

7.2.3 Customer selected PIN

When a reference PIN is a "customer selected PIN" the value shall be selected by the customer. In this case the issuer shall provide the customer with the necessary selection instructions and warnings (see annex H).

NOTE 8 To the issuer, a customer selected PIN is random in value.

7.3 PIN delivery and issuance

All PIN issuance functions involving issuer personnel shall be under dual control.

The PIN shall never be retrieved and deciphered or regenerated to be recorded, processed, displayed, or printed except in a secure PIN mailer (or its equivalent).

At no point in the delivery process shall the PIN appear in plain text where it can be associated with a customer's account.

7.3.1 Delivery of an assigned PIN

A PIN assigned by an issuer shall be conveyed to the customer by means of a PIN mailer.

The PIN mailer shall be printed in such a way that the plain text PIN cannot be observed until the envelope is opened. The envelope shall display the minimum data necessary to deliver the PIN mailer to the correct customer. A PIN mailer shall be constructed such that it is highly likely that accidental or fraudulent opening will be obvious to the customer. The issuer shall warn the customer not to use a PIN that is contained in an opened or tampered PIN mailer and to notify the issuer of such an event.

NOTES

9 The envelope or its contents may contain "residue of the PIN" (e.g. carbon paper), and the issuer should warn the customer that after memorizing the PIN, he should destroy the mailer completely or keep the mailer in a safe place.

10 Multiple cards may be in issue on the same account, each with a different PIN. If so, the outside of the PIN mailer may have to display details of the customer's identification to facilitate correct delivery.

The PIN and card shall not be mailed in the same mailer nor at the same time.

7.3.2 Delivery of customer selected PIN

A PIN selected by the customer shall be conveyed to the issuer using one of the following techniques:

a) initial PIN selection at an issuer's location (see 7.3.2.1);

b) PIN selection by mail (see 7.3.2.2).

7.3.2.1 PIN selection at an issuer's location

PIN selection shall be accomplished at an issuer's location via a PIN pad complying with the requirements of table 2. Selection and entry of the PIN shall not involve the customer disclosing the PIN to any issuer's employee or third party. The following procedure shall be applied.

a) An authorized employee shall obtain proper identification of the customer.

b) The system shall require identification and authorization of the issuer's employees.

c) The PIN selection process shall be enabled by an authorized employee. The process shall be terminated by the completion of a PIN selection.

d) The authorized employee's identification together with the date and the time shall become a part of the transaction record.

7.3.2.2 PIN selection by mail

PIN selection by mail shall only be accomplished by the use of a form containing a control number and space for a selected PIN. The control number shall not disclose the account number. Any cryptographic key used to generate a control number shall not be used for any other purpose and shall be managed in accordance with annex B. The completed form shall not contain any information which relates the PIN to the customer's name, address, or account number. The following procedures shall apply.

a) The mailer to the customer shall contain the PIN selection form and instructions.

b) The mailing shall be in accordance with the procedures defined in 7.3.1, treating the control number as the PIN.

c) The customer shall be instructed to write the PIN on the form, not to write any other information on the form unless specifically requested, not to enclose any other correspondence, and to return the form to the stated address. A special pre-addressed envelope should be used.

d) The processing of received PIN selection forms shall only be by authorized employees of the issuer.

NOTE 11 The control number may be the reversibly enciphered account number. Some issuers instruct the customer to enter an enciphered PIN on to the form.

7.4 PIN change

PIN change shall be performed through the issuer's system in accordance with the requirements of 7.3; it shall not be performed in an interchange environment.

7.4.1 PIN change at an attended terminal

The procedure for PIN change at an attended terminal shall be the same as specified for PIN selection in 7.3.2.1.

7.4.2 PIN change at an unattended terminal

The procedure for PIN change at an unattended terminal in the issuer's system shall require the current PIN to be entered and verified before selection and activation of the replacement customer selected PIN.

NOTE 12 The new PIN should be entered twice and both entries should be identical.

7.4.3 PIN change by mail

The procedure for PIN change by mail shall be the same as specified for PIN selection in 7.3.2.2.

7.4.4 Replacement of forgotten PIN

Replacement of a forgotten PIN shall be performed through the issuer's system; it shall not be performed in an interchange environment. The procedures used to replace a forgotten PIN shall follow those covered in 7.3.

Where an assigned PIN has been forgotten and the effect is to generate a PIN mailer communicating the same, or a newly assigned PIN value, the requirements of 7.3.1 shall apply.

7.4.5 Replacement of compromised PIN

When a PIN is believed to have been compromised, it shall be deactivated as soon as possible (see 7.8) and the customer informed of a replacement value or given the opportunity to select one. A replacement PIN shall not be intentionally the same as the original PIN. Activation of a replacement PIN may be implicit or explicit (see 7.6).

When an assigned derived PIN is believed to have been exposed, at least one data element used in deriving the PIN shall be changed and a new PIN derived and issued. This may require that any corresponding card be re-issued or re-encoded and that the old card be blocked from use.

7.5 Disposal of waste material and returned PIN mailers

Issuers shall ensure that adequate security measures are taken over the internal handling and disposal of returned PIN mailers and any waste material associated with the initial printing of PIN mailers.

NOTE 13 Consideration should be given to different return addresses in case of non-delivery for card and PIN mailers.

7.6 PIN activation

A PIN may be activated either implicitly or explicitly. Under a system of implicit PIN activation the issuer assumes successful PIN delivery, unless advised to the contrary.

When a PIN is to be explicitly activated, the issuer shall not activate the PIN until the customer has returned a signed, and subsequently verified, receipt. The receipt shall not contain the PIN.

7.7 PIN storage

A PIN stored in the computer files of the issuer shall be enciphered as specified in 6.2.

PIN encipherment (reversible or irreversible) shall incorporate the account number (or other data) such that the verification process would detect substitution of one value for another stored value.

When the PIN (assigned or customer selected) is stored on a card, it shall never be stored as clear text. If the PIN is to be stored on the card, it shall be enciphered (e.g. PIN offset).

7.8 PIN deactivation

Responsibility for PIN deactivation rests with the issuer. An issuer shall deactivate a PIN if any of the following occurs:

a) the PIN is compromised (or suspected to be compromised);

b) all of the customer's accounts associated with the PIN are closed;

c) the customer requests deactivation of the PIN;

d) the lifetime of the PIN ends.

In the case of PIN compromise, the customer shall be advised of the action taken.

The issuer shall take appropriate measures to ensure that the deactivated PIN cannot subsequently be used with its associated account number.

NOTE 14 Examples of such measures are

a) erasure of the deactivated PIN from the issuer's records;

b) blocking access to the account.

8 Techniques for management/protection of transaction-related PIN functions

8.1 PIN entry

Responsibility for protecting the PIN during the entry process rests with the customer, the card acceptor, and the acquirer or its agent.

The first digit entered into the PIN pad shall be the high-order digit (left-most). The last digit to be entered shall be the low-order digit (right-most).

Equipment used for interchange shall support entry of a 4 to 12 character PIN.

8.2 Protection of PIN during transmission

A PIN shall be protected during transmission (including, for example, storage at network nodes) by one or both of the following means:

a) provision of physical protection (see 6.3);

b) encipherment of the PIN (see 6.2).

Whenever it is necessary to decipher a PIN during transmission, for instance to translate from one PIN format to another or to change the encipherment key used, the PIN shall be contained within a physically secure device.

8.3 Standard PIN block formats

This subclause specifies the construction of a 64-bit block of PIN data and includes the number, position and function of the bits.

The most significant 4 bits of the block form the control field. The following values are assigned:

0000 — Format 0 as defined in 8.3.1.

0001 — Format 1 as defined in 8.3.2.

0010 through 0111 — For allocation by ISO/TC 68.

1000 through 1011 — Reserved for allocation by national standards organizations.

1100 through 1111 — Allocated for private use.

8.3.1 Format 0 PIN block

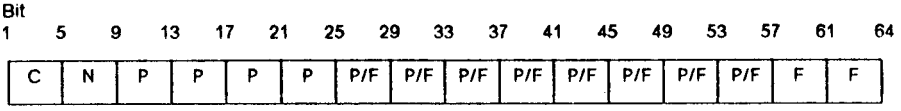
This PIN block is constructed by modulo-2 addition of two 64-bit fields: the plain text PIN field and the account number field. The formats of these fields are described in 8.3.1.1 and 8.3.1.2 respectively.

The format 0 PIN block shall be reversibly enciphered when transmitted.

In international interchange, the format 0 PIN block should be used when the PAN is available.

8.3.1.1 Plain text PIN field

The plain text PIN field shall be formatted as follows:



where

C = Control field — Shall be 0000.

N = PIN length — 4-bit binary number with permissible values of 0100 (4) to 1100 (12).

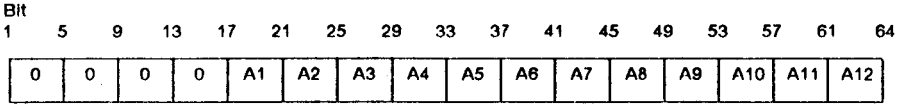
P = PIN digit — 4-bit field with permissible values of 0000 (zero) to 1001 (9).

P/F = PIN/Fill digit — Designation of these fields is determined by the PIN length field.

F = Fill digit — 4-bit field value 1111 (15).

8.3.1.2 Account number field

The account number field shall be formatted as follows:



where

0 = Pad digit — A 4-bit field. The only permissible value is 0000 (zero).

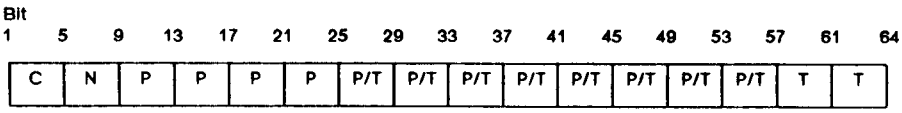
A1 ... A12 = Account number — Content is the 12 right-most digits of the primary account number (PAN), excluding the check digit. A12 is the digit immediately preceding the PAN's check digit. If the PAN excluding the check digit is less than 12 digits, the digits are right justified and padded to the left with zeroes. Permissible values are 0000 (zero) to 1001 (9).

8.3.2 Format 1 PIN block

This PIN block is constructed by concatenation of two fields: the plain text PIN field and the transaction field. It should be used in situations where the PAN is not available.

The format 1 PIN block shall be reversibly enciphered when transmitted.

The format 1 PIN block shall be formatted as follows:



where

C = Control field — Shall be binary 0001.

N = PIN length — 4-bit binary number with permissible values 0100 (4) to 1100 (12).

P = PIN digit — 4-bit field with permissible values 0000 (zero) to 1001 (9).

P/T = PIN/Transaction digit — Determined by PIN length.

T = Transaction digit — 4-bit binary number with permissible values of 0000 (zero) to 1111 (15).

The transaction field is a binary number formed by [56 – (N*4)] bits. This binary number shall be unique (except by chance) for every occurrence of the PIN block and can, for example, be derived from a transaction sequence number, time stamp, random number, or similar.

NOTE 15 The transaction field should not be transmitted and is not required in order to translate the PIN block to another format since the PIN length is known.

8.4 Other PIN block formats

If the PIN block cannot be constructed in the terminal to comply with the format shown in 8.3 then alternative methods shall be employed in the local network so that the same PIN when associated with different accounts shall produce a different enciphered result.

The acquirer shall ensure the secure translation of a non-standard PIN block format to a standard PIN block format (see 8.3).

8.5 PIN verification

Responsibility for PIN verification shall rest with the issuer although the verification function may be delegated to another institution.

NOTE 16 Some guidance on PIN verification techniques is provided in annex C.

8.6 Journaling of transactions containing PIN data

Terminals or other nodes in networks may be required to journal (i.e. to record the full text of) transaction messages. Messages journalled shall not contain a plain text PIN. It is permissible to journal messages containing a PIN enciphered in accordance with 6.2 if and only if the prevention of disclosure of the PIN decipherment key(s) in any form can be assured for the lifetime of the PIN.

NOTES

17 A PIN should not be stored for longer than necessary.

18 Cardholders' claims related to PIN disclosure and/or fraudulent use should be recorded in such a way as to identify the possible source of a failure and/or misuse.

9 Approval procedure for encipherment algorithms

Before an encipherment algorithm can be added to ISO 9564-2, it shall satisfy the following basic requirements:

a) it shall be designed to serve a purpose not already covered by ISO 9564-2 (for example, for a different market; to show significant cost savings in implementation or in operation; or to offer a measurably greater degree of protection);

b) it shall be sufficiently secure, reliable and stable to serve its stated purpose. Algorithms shall be approved in accordance with the requirements of annex A.

Annex A
(normative)

Procedure for approval of an encipherment algorithm

The following procedure for approval of an encipherment algorithm for use with this part of ISO 9564 shall be used by ISO/TC 68.

A.1 Justification of proposal

ISO/TC 68 shall require the originator to justify a proposal by describing

a) the purpose the proposal is to serve;

b) how this purpose is better achieved by the proposal than algorithms already in ISO 9564-2;

c) additional merits not described elsewhere;

d) experience in use with the new algorithm.

A.2 Documentation

The proposed algorithm shall be completely documented when submitted for consideration. The documentation shall include

a) a full description of the algorithm proposed;

b) a clear acknowledgement that the algorithm satisfies, or is compatible with, all the requirements contained in this part of ISO 9564;

c) a definition and explanation of any new terms, factors, or variables introduced;

d) a step-by-step example illustrating the encipherment and decipherment computation;

e) detailed information on any prior testing to which the proposed algorithm has been subjected, particularly concerning its security, reliability and stability. Such information shall include an outline of the testing procedures used, the results of the tests, and the identity of the agency or group performing the tests and certifying the results (that is, sufficient information shall be provided to enable an independent agency to conduct the same tests and to compare the results achieved).

A.3 Public disclosure

Any algorithm submitted for consideration shall be free of security classification. If copyright or patent application has been made on the algorithm, the originator shall submit the appropriate letter stating that the originator is willing to grant a licence under these copyrights and patents on reasonable and non-discriminatory terms and conditions to anyone wishing to obtain such a licence to allow free and unconditional use by testers, users and suppliers of supporting equipment or material. All documentation and information submitted with the request for consideration of the algorithm shall be considered public information available to any individual, organization or agency for review, testing and usage.

A.4 Examination of proposals

ISO/TC 68 shall examine and prepare a report on each new proposal submitted. The report shall normally be sent to the ISO/TC 68 Secretariat within 180 days of receipt of the proposals (see A.5). The report shall state whether the proposal is adequately documented, whether it has been properly tested and certified already, and

whether the proposed algorithm satisfies the conditions and requirements of this part of ISO 9564. The examination may also include submission of the proposal for public review (see A.5).

The convener shall determine in each case whether such report and recommendations are best prepared by correspondence between the members or by a meeting. If a meeting is to be held, at least 60 days notice of the date shall be given and of the papers to be dealt with at the meeting.

Where a majority of members of ISO/TC 68 recommends the rejection of the proposal, the Secretariat shall notify the originator, in writing, advising of the rejection and the reasons for it.

A.5 Public review

ISO/TC 68 shall forward proposals which it considers should be accepted (and which have not already been subjected to extensive testing or experience) to selected agencies or institutions with an international reputation in this field. These agencies and institutions will be requested to examine and report on the proposals within 90 days of receipt.

NOTE 19 This period of public review may extend the 180 days allowed for ISO/TC 68 to prepare its overall report on the proposal (see A.4).

A.6 Appeal procedure

Originators whose proposals are rejected by ISO/TC 68 (see A.4) may ask the Secretariat of ISO/TC 68 to have the proposals subjected to public review (see A.5) if this has not already been done. If, following submission of the public review reports, ISO/TC 68 still recommends rejection, the originator may request the ISO/TC 68 Secretariat to circulate the proposal, together with copies of all relevant reports on it, for ballot by P-members of the subcommittee whose ruling in the matter shall be final.

A.7 Incorporation of new encipherment algorithm

New encipherment algorithms recommended for acceptance by ISO/TC 68, together with relevant reports on them, shall be circulated for letter ballot by the Secretariat of ISO/TC 68 to all P-members of the subcommittee. Proposals approved as a result of this process shall be forwarded to the Secretariat of ISO/TC 68 for action under the abbreviated procedure to amend an existing International Standard (see *IEC/ISO Directives, Part 1: Procedures for the technical work*, 1989). Once approval is given, the new encipherment algorithm shall be added to ISO 9564-2.

A.8 Maintenance

An algorithm approved by the method described in this part of ISO 9564 shall be reviewed at intervals of not greater than 5 years.

Annex B
(normative)

General principles of key management

ISO/TC 68/SC 6 is in the process of drafting an International Standard dealing with the subject of key management which is to be used in conjunction with this part of ISO 9564. It is intended that this annex will be superseded by the new key management International Standard when it is available.

Any PIN enciphering key shall be managed in accordance with the requirements of this annex.

NOTE 20 Cryptographic keys may be hierarchically structured. Various environments may require different levels of hierarchy, e.g. some terminals might require 2 levels. An example of a 3 level hierarchy is as follows.

a) At the highest level of the hierarchy is the host master key. This key or a variant of the key is used to encipher all keys at the next level.

b) At the next level are key enciphering keys. These are used to encipher PIN enciphering keys (and data enciphering keys) in storage.

c) At the bottom level are working keys (e.g. PIN enciphering keys, used to encipher a PIN for storage or transmission).

B.1 Key generation for secret key algorithms

Keys shall be generated by a random or a pseudo-random process, such that it is not feasible to predict any key or to determine that certain keys are more probable than other keys from the set of all possible keys.

B.2 Protection against key disclosure

A cryptographic key shall only exist in the following forms:

a) as at least two key components controlled by the process of dual control and split knowledge. Each key component shall be generated as specified by B.1. Each key component shall contain the same number of bits as the key itself.

   The formation of a key from the key components shall depend upon the interaction of all key components, e.g. by modulo-2 addition.

   If a key component is in human comprehensible form (e.g. when printed in plain text inside a mailer) it shall be known to only one authorized employee, at only one point in time, and only for as long as is required for the key component to be entered into a device or system complying with 6.3. It shall be ensured that the authorized employee who handles this component is the only person that has knowledge of its value and access to the component. This person shall not have access to another component that constitutes the same key.

b) in a device or system complying with the requirements of 6.3.1 or 6.3.3 or in an issuer's facility complying with 6.3.2.

c) enciphered using a key enciphering key.

B.3 Protection against key substitution

Keys and related keying material shall be transported and stored in such a manner as to protect them against modification or substitution.

NOTES

21 If action to prevent substitution is not taken an adversary might substitute a key with a known value for a key whose value is not known.

22 Protection may be provided using one of the following methods:

a) by a combination of physical protection complying with 6.3 and procedural techniques which prevent such substitution;

b) by utilization of key notarization techniques;

c) by ensuring that it is not possible to know both a plain text value and its corresponding cipher text enciphered under a key enciphering key.

If it is believed or known that key substitution has occurred, both the key and any associated key enciphering key shall be deactivated and changed.

B.4 Restrictions on use of PIN protection keys

A key which is used to encipher a PIN shall never be used for any other cryptographic purpose. A key which is used to protect the PIN enciphering key shall never be used for any other cryptographic purpose. However, variants of the same key may be used for different purposes.

B.5 Limiting the effects of a key compromise

The following requirements are necessary to prevent the compromise of the key or keys in one cryptographic device from compromising any other cryptographic device.

Any key enciphering key or any transaction PIN enciphering key shall only exist at the minimum number of locations consistent with the effective operation of the system.

NOTE 23 This will in many cases be only two locations but where, for instance, resilient networks with alternative routeing are used, or hot-back-up is employed, then these keys must of necessity be held at more than two locations.

Any key used by a PIN entry device not complying with 6.3.1 shall not be shared with any other PIN entry device.

Only an issuer or its agent may have access to any key used to encipher or derive a reference PIN.

No cryptographic key shall, except by chance, be equal to any other cryptographic key. Except for the variant of a key, the irreversible transformation of a key, or keys enciphered under a key, knowledge of one cryptographic key must provide no information about any other cryptographic key.

The irreversible transformation of a key shall be used only at the same level as the original key, or the level immediately below that of the original key.

The variant of a key may be used only in those devices which possess or possessed the original key.

B.6 Key replacement

A cryptographic key shall be replaced with a new key whenever the compromise of the original key is known or suspected. Knowledge of the original key shall not provide any information which might be feasibly used to determine the replacement key. The replacement key shall not be a variant of the original key, or an irreversible transformation of the original key.

A cryptographic key shall be replaced with a new key within the time deemed feasible to determine the key by exhaustive attack.

Annex C
(informative)

PIN verification techniques

This annex describes three basic PIN verification techniques, by means of which the validity of the PIN entered at a terminal can be verified. These processes are

a) PIN verification at a terminal,

b) PIN verification by an issuer, and

c) PIN verification by an institution other than an issuer.

The principle behind all three techniques is to compare the PIN as keyed in (the transaction PIN) with reference data originating from the issuer, e.g. the reference PIN. For a comparison to be valid the transaction PIN or the reference data, or both, may require transformation, for instance by encipherment, decipherment or translation. Irreversible encipherment, for example using a one-way function, may provide a higher level of security when reference data are exchanged.

The method used for transmitting and storing data may influence the technique selected for PIN verification. In addition, each of the described techniques involves different levels of complexity of implementation and of exposure to risk.

C.1 PIN verification at a terminal

To achieve PIN verification at a terminal the device needs to have access to the reference data (the transaction PIN will be available at the terminal as a matter of course). The reference data will be either

a) obtained or derived from the customer's card, or

b) obtained/transmitted from the issuer.

Where the reference data are obtained from the customer's card the disclosure of the secret cryptographic keys utilized within the terminal may expose all of the PINs of those issuers.

C.2 PIN verification by the issuer

Where the verification of a PIN is carried out by the issuer concerned, the issuer needs to have access to the transaction PIN or a derivative thereof (the reference data will be available to the issuer as a matter of course). The enciphered transaction PIN, therefore, needs to be transmitted from the terminal to the issuer.

C.3 PIN verification by an institution other than an issuer

PIN verification by an institution other than an issuer is carried out neither at the terminal at which the transaction PIN is entered, nor by the issuer. Both items of data required for the comparison need to be provided to the institution concerned.

Thus, the transaction PIN, or a derivative, needs to be transmitted from the terminal. The reference data may be either obtained from the issuer or derived from data on the customer's card and transmitted with the transaction PIN (or a derivative). When this technique is used the PIN security of the issuer depends upon the integrity of the facility of the institution concerned.

Annex D
(informative)

PIN entry device

D.1 General

Subclause 6.3.3 of this part of ISO 9564 allows a PIN entry device (especially for point-of-sale usage) to have a lesser degree of physical security than does a "physically secure device" provided that several conditions are met. The most significant of these conditions is that no information remaining in the device at the end of a transaction could, if ascertained, be used to determine any PIN which had been entered into the device, even given a knowledge of all relevant data which have ever been available external to this device. Assuming that the device enciphers the PIN using DEA-1, this condition requires that the cryptographic key used for PIN encryption changes after every transaction, and that there be no feasible way to determine any past key given the knowledge of the key or keys currently stored within the device, as well as the knowledge of any data which had been transmitted to or from the device while in operational service.

The commonly used "master key, working key" technique does not meet this condition, even if a new working key enciphered under the master key were transmitted to the device after every transaction. A knowledge of the master key, together with a knowledge of the data which had been transmitted to and from the device, would enable decipherment of the enciphered working keys transmitted to the device, which in turn would allow the decipherment of any enciphered PIN transmitted from the device.

A recommended method of meeting the above condition is the generation of a new PIN encipherment key by the "irreversible transformation" of the current PIN encipherment key as soon as the transaction using the current key has been completed. (If key "X" is the irreversible transformation of key "Y", this means that there is no feasible way to determine "Y" given a knowledge of "X".) In this way the device has a unique key for every transaction, but there is no feasible way to determine any previous key given a knowledge of the current key.

In one implementation of an irreversible transformation methodology the transformation process utilizes the data which are normally discarded when a Message Authentication Code (data field used to verify the authenticity of a message) is generated (MAC residues). This cryptographically links transactions together, providing a form of "audit trail". In those situations in which a "card key" (a derivative of untransmitted card data) is present, security can be enhanced by including the "card key" in the irreversible transformation process.

The acquirer must be able to determine the current key in each of many (perhaps tens of thousands) of PIN entry devices. There are a number of techniques by which this can be achieved. Three techniques are described in D.2 to D.4.

D.2 Enciphered key stored in database of acquirer

The acquirer's facility is assumed to contain a physically secure device, and a non-secure database. The current key for each PIN entry device is stored in this database in enciphered form, the key enciphered key being known only within the physically secure device. When a transaction is received from a PIN entry device, the acquirer first locates the enciphered key for this device in the database. The appropriate transaction data and this enciphered key are transferred to the physically secure device, which deciphers the latter in order to determine the device's current key. After the physically secure device has determined that the key from the database is the same as the key in the PIN entry device (e.g. by examining the deciphered PIN block, or by verifying a Message Authentication Code which is based on a key related to the PIN encipherment key), the physically secure device performs the same irreversible transformation that the PIN entry device will perform to produce the key for the next transaction. It then enciphers this key, and returns it for storage in the database.

It may be necessary for the database to store both the enciphered key for the current transaction and the enciphered key for the next transaction. This provides for the possibility that the current transaction might fail to complete, so that the PIN entry device will retain the current key rather than irreversibly transform the current key to generate a new key.

D.3 Enciphered key stored in terminal or PIN entry device

This approach operates essentially as described in D.2 except that there is no database of enciphered keys. Instead of being stored in a database, the enciphered next key for a PIN entry device (enciphered under a key encipherment available only within the acquirer's physically secure device) is transmitted back to the associated terminal in the transaction response message, and stored there. This enciphered key is included in the next transaction request message from the terminal, so is available to the acquirer's physically secure device when it processes this transaction. Note that the PIN entry device is unable to decipher this enciphered key, but rather obtains this key by irreversibly transforming the previous key.

When this technique is utilized, message authentication is highly desirable to ensure that the enciphered version of the new key has been correctly received by the terminal from the acquirer's facility. The PIN entry device should ensure this before irreversibly transforming the current key to produce the new key.

Eliminating the database of enciphered keys from the acquirer's facility reduces failure-recovery problems. With a database of dynamically changing enciphered keys, the acquirer must provide a failure-recovery mechanism so that the latest version of each enciphered key can be recovered if there is a failure of the storage medium which holds this database.

D.4 Derived unique key per transaction

This technique is similar to the technique described in D.3 in that there is no need to maintain a database of enciphered keys. However, this technique does not require transmission of the enciphered key back to the terminal, and so is essentially transparent to the acquirer's on-line processing activities. In addition, it does not inherently require that message authentication be used.

In this technique a non-secret "key serial number", which increments on each transaction, is transmitted from the PIN entry device with each enciphered PIN. The acquirer's physically secure device is able to compute cryptographically the current PIN-entry-device key given only a secret "derivation key", common to many PIN entry devices, but residing in none of them, and the "key serial number" included with the current transaction.

In order to reduce the computational task required of the acquirer's physically secure device, the key for the current transaction is the non-reversible transformation of the key used for some previous transaction, but not necessarily the immediately preceding one. In a possible implementation of this technique the acquirer can compute cryptographically the PIN entry device's current key using a relatively small number of encipherment operations. For example, if the PIN entry device can utilize 1 million unique keys, the acquirers can compute the current key in no more than 12 encipherment operations.

Annex E
(informative)

Example of pseudo-random PIN generation

This example uses the Data Encryption Algorithm — ANSI X3.92:1981. eX(Y) represents the DEA encipherment of Y under key X in the ECB mode. Let K be a secret DEA-1 key and let S be a seed value. S may be initially set to any number. Let DT be a date-time word and also let XOR represent the bit-by-bit Exclusive or operation. A 64-bit intermediate vector I and a 64-bit pseudo-random vector R are generated as follows:

I = eK (DT)

R = eK (I XOR S)

and a new S is given by

S = eK (R XOR I)

As with all random number generators, each implementation should be periodically checked to ensure proper functioning.

The PIN digits are then derived from R by the following procedure.

Consider R, a 64-bit cipher block, as 16 hexadecimal digits. Scan these digits, skipping any digits greater than 9, until the required number of decimal PIN digits has been found. If all 16 cipher digits have been scanned without finding the required number of decimal PIN digits, find the remaining required digits by rescanning the cipher digits, considering only digits greater than 9 and subtracting 10 from each.

NOTE 24 Warning, this technique yields digits with a negligible bias towards the digits 0 to 5.

Annex F
(informative)

Additional guidelines for PIN pad design

F.1 Introduction

This annex describes features such as function keys and the design of a PIN pad installation. As such it supplements the requirements given in clause 5 of this part of ISO 9564.

F.2 Key layout

While it is particularly important that the layout of the numeric keys on a PIN pad is fixed, it is extremely desirable that the overall layout, including any function keys, is standardized in order to help the customers in their use of the PIN pad. Common layouts promote familiarity and consistency of operation, thereby reducing errors in PIN entry.

As well as maintaining a constant layout, function keys should be given an unambiguous and constant meaning. The three typical functions initiated by individual keys are

— "enter" or "complete entry";

— "clear" this entry;

— "cancel" transaction.

In addition to any engravings indicating the function of the keys, the following use of colours on the keys is recommended:

— Green — "Enter"

— Yellow — "Clear"

— Red — "Cancel"

Where the function keys are arranged in a vertical column, they should be located to the right of the numeric keys with the "cancel" key at the top, "clear" in the middle and "enter" at the bottom. When arranged horizontally the same order should be used, with the "cancel" key on the left, and the "enter" key on the right, and the "clear" key in the middle.

EXAMPLE 1 — The numeric PIN pad with two horizontally placed function keys.

1	2	3
4	5	6
7	8	9
RED	0	GREEN

EXAMPLE 2 — ANSI alpha-numeric PIN pad with vertically placed function keys.

QZ 1	ABC 2	DEF 3	RED
GHI 4	JKL 5	MNO 6	YELLOW
PRS 7	TUV 8	WXY 9	GREEN
	0		

EXAMPLE 3 — CCITT alpha-numeric PIN pad with vertically placed function keys.

1	ABC 2	DEF 3	RED
GHI 4	JKL 5	MN 6	YELLOW
PRS 7	TUV 8	WXY 9	GREEN
	OQ 0		

F.3 Privacy during PIN entry

Visual observation of the PIN is the most common way that a PIN is compromised. Privacy during PIN entry may be achieved by providing a cowl over the keys or by positioning the PIN pad so that during PIN entry the keys are shielded by the customer's body, for example, when using a hand-held PIN pad. Special consideration should be given to prevent the possible recording of the PIN entry by video cameras.

F.4 Alpha-to-numeric mapping

The following describes the relationship between the customer-known character set (which may be alphabetic, numeric, or both) and the internal binary codes. Alphabetic characters are only synonyms for decimal digits and are not distinguishable by the terminal or network. Tables F.1 and F.2 show the ANSI and CCITT alpha-numeric mapping.

Table F.1 — ANSI alpha-to-numeric mapping

Customer-known alphabetic	Customer-known decimal	Internal binary
	0	0000
QZ	1	0001
ABC	2	0010
DEF	3	0011
GHI	4	0100
JKL	5	0101
MNO	6	0110
PRS	7	0111
TUV	8	1000
WXY	9	1001

NOTE — ANSI prescribes no alpha-to-numeric character mapping for the zero digit.

Table F.2 — CCITT alpha-to-numeric mapping

Customer-known alphabetic	Customer-known decimal	Internal binary
OQ	0	0000
	1	0001
ABC	2	0010
DEF	3	0011
GHI	4	0100
JKL	5	0101
MN	6	0110
PRS	7	0111
TUV	8	1000
WXY	9	1001

NOTE — Card issuers should be aware that the mapping of the alphabetics "O", "Q", and "Z" to decimal digits vary internationally. It is recommended that if non-numeric PINs are to be used in international interchange, then it is the responsibility of the issuer to advise their customers accordingly.

Annex G
(informative)

Guidance on clearing and destruction procedures for sensitive data

G.1 Purpose

To establish guidance on uniform erasing (zeroizing) (e.g. degaussing, erasing and overwriting), clearing and destruction procedures for storage material used so that unauthorized access to or compromise of the data is prevented.

G.2 General

Owing to the physical properties and retentive capabilities of storage media and devices (e.g. magnetic cores, drums, disks and various microelectronic circuits) used to store, record or manipulate sensitive data, special precautions should be taken to safeguard against the compromise of possible residual information. This annex presents recommended procedures for such zeroization or destruction.

G.3 Cathode ray tube (CRT)

A display CRT can be considered zeroized if, after visual inspection, it is determined that no sensitive information has been etched into the CRT phosphor coating.

If there is any doubt after inspection of the screen, the CRT surface should be highlighted by filling the screen with vectors to create a raster effect to light up the entire screen. The brightness of the raster can be varied with the intensity control. Any burns or uneven illumination of the phosphor coating that could be considered compromising should then be easily detected. Random burns on the CRT should not necessitate automatic classification of the CRT as containing sensitive information.

Should any area of the CRT be determined to contain sensitive information, the CRT should remain classified at the highest level of residual information.

If the CRT becomes defective and cannot be purged of sensitive information, it should be destroyed.

G.4 Magnetic core memory

To zeroize a magnetic core memory, overwrite all data bit locations. All data bit locations should be set to zeros and verified for successful entry; then all locations should be set to ones and the verification repeated. This overwrite procedure (with random hard copy readout or other equivalent verification at the conclusion) should be executed alternately with zeros and ones for 1 000 cycles. Finally, non-sensitive, arbitrary data should be written in all data bit locations and left in the core.

Alternative procedures are as follows.

a) The magnetic core memory should be destroyed by pulverizing, melting or incinerating.

b) Expose all cores to a recommended magnet. The magnet should be held within 1 cm of each core.

G.5 Disk pack

To zeroize magnetic disk packs, overwrite all data bit locations three times by setting zeros and ones alternately. Verify successful entry of the overwrites through a random hard copy readout or equivalent verification. Write non-sensitive arbitrary data on all data locations on all tracks of the disk and leave them there.

If the disk has failed in such a way that it cannot be overwritten or the overwrite cannot be verified, clear the disk by exposing the recording surface to a permanent magnet assembly.

Cover the magnet assembly with a lintless wiping tissue to prevent damage to recording surfaces. Wipe the entire surface at least three times with the magnet.

Alternative procedures are as follows.

a) Apply an emery wheel or sander to the recording surface of an inoperative disk. Ensure that the entire surface is completely removed prior to disposal.

b) The resin binder and ferric oxide surface can be completely removed/stripped (chemically destroyed) from the disk with concentrated hydrochloric acid (55 % to 58 %).

c) Melt down the disk pack.

G.6 Drum

To zeroize a magnetic drum, overwrite all data bit locations three times by setting zeros and ones alternately. Verify successful entry of the overwrites through a random hard copy readout or other equivalent verification.

Write non-sensitive arbitrary data on all data locations, verify that the data have been written to these locations, and leave them there.

If the drum has failed in such a way that it cannot be overwritten or the overwrite cannot be verified, zeroize the drum by exposing the recording surface to a permanent magnet assembly. Cover the magnet with a lintless wiping tissue to prevent damage to the recording surface. Wipe the entire surface at least three times with the magnet. Ensure that all recording areas of the drum are exposed to the active area of the magnet assembly.

G.7 Magnetic tapes

Magnetic tapes should be zeroized with a degausser. Magnetic tapes may be cleared by overwriting one time with any one character. However, cleared magnetic tapes should be safeguarded, controlled, and marked at the level commensurate with the most sensitive information recorded on them before they were released for destruction. Before release of a zeroized magnetic tape, it should be subjected to two degaussing cycles and removed from the reel, then destroyed by disintegration into pieces 9 mm, or smaller, or incineration.

G.8 Internal memory, buffers, and registers

Internal memory, buffers, and registers should be zeroized initially by use of a hardware clear switch or power-on/off reset cycle, and then by overwriting all data bit locations with continuously changing random data for 1 000 cycles. Periodic verification should be made that the method(s) are working correctly. Verify successful entry of the overwrites through a random hard copy readout or through other equivalent verification. Finally, all locations should be overwritten with non-sensitive, random data and verified.

G.9 Semiconductor memory

a) Random Access Memory (RAM) should be initialized by use of a power-on/off reset cycle. Overwrite the storage area by alternately setting each data bit location to all zeros then all ones for 1 000 cycles. Periodic verification should be made that the method is working correctly. Verification may take the form of random sampling or use of a read and compare program. Finally, all locations should be overwritten with non-sensitive data and verified.

b) Erasable Programmable Read Only Memory (EPROM) should be initialized by optical ultraviolet erasing the entire array. Zeroization should be verified. All storage locations should be overwritten with non-sensitive random data and verified.

c) Electrically Alterable Read Only Memory (EAROM) should be initialized by pulsing all gates. Zeroization should be verified. All storage locations should be overwritten with non-sensitive random data and verified.

d) Electrically Erasable Programmable Read Only Memory (EEPROM) should be initialized by pulsing the erase control gate. Zeroization should be verified. All storage locations should be overwritten with non-sensitive random data and verified.

e) Read Only Memory (ROM) is physically programmed during manufacture. Physical destruction is the only recommended method to ensure erasure.

G.10 Paper materials

Paper materials should be destroyed by burning, pulverizing, or crosscut shredding. When material is pulverized, all residue should be reduced to pieces 5 mm or smaller. When material is burned, the residue should be reduced to white ash.

G.11 Platens and ribbons

The printer platen and ribbon should be removed from a printer before the printer is released. Platens (only the rubber surface should be physically removed for destruction) and ribbons should be destroyed (e.g. by incineration).

Annex H
(informative)

Information for customers

The issuer needs to provide those customers having a card and an associated PIN with information that emphasizes the importance of the PIN and PIN security. In particular, the following information needs to be provided.

a) The customer should never orally communicate the plain text of a PIN to any person or device.

b) The customer should never enter a PIN by means of the keypad of a telephone except where the telephone complies with the requirements for PIN pads specified in clause 5, and for communication security specified in 8.2.

c) When the customer selects or changes the PIN, they should be advised of the following:

   1) that the selected PIN should not have a value that is readily associated with the customer (e.g. surname, telephone number, birth date);

   2) that the selected PIN value should not comprise

      — a sequence from the associated account number

      — strings of the same number

      — historically significant dates

      — an alpha-based string (word) of less than 6 characters

      — a numeric string (number) of less than 4 characters

   3) that unsolicited information should not be included on or with the returned PIN selection form.

d) When a customer-initiated PIN change is put into effect, a notification of the change, but not the PIN value, should be mailed to the customer. The notification should contain instructions to contact the issuer immediately if the change had not been requested by the customer.

e) The customer should be advised to enter the PIN in a way that cannot be observed by others.

f) Customers whose issuers support alpha-numeric PIN selection should be advised by their issuer that it may not be possible to use other than a numeric PIN value on systems other than the issuers.

g) The customer should be advised to memorize the PIN and not to write it on the card.

h) Customers should be advised to notify the issuer if a PIN mailer has been previously opened or not received intact.

(*Continued from second cover*)

The International Standard ISO 8583 has been revised and is published in three parts. Part 1 of this International Standard is currently published as:

ISO 8583 : 1993	Financial transaction card originated messages — Interchange message specifications

This standard is again being revised at ISO level and the revised version, as and when published, will be considered for adoption as an Indian Standard.

Part 2 and Part 3 of this International Standard have been adopted as Indian Standards and their details are given below:

IS 14943 (Part 2) : 2001/ ISO 8583-2:1998	Financial transaction card originated messages — Interchange message specifications: Part 2 Application and registration procedures for institution identification codes (IIC)
IS 14943 (Part 3) : 2001/ ISO 8583-3:1998	Financial transaction card originated messages — Interchange message specifications: Part 3 Maintenance procedures for codes

Annexes A and B form an integral part of the adopted standard. Annexes C, D, E, F, G and H of the adopted standard are 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 (179).

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