INTERNATIONAL STANDARD

ISO 9564-1

Second edition
2002-04-15

Banking — Personal Identification Number (PIN) management and security —

Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems

Banque — Gestion et sécurité du numéro personnel d'identification (PIN) —

Partie 1: Principes et exigences de base pour la gestion du PIN en ligne dans les systèmes ATM et POS

Reference number
ISO 9564-1:2002(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Page

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

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

Attention is drawn to the possibility that some of the elements of this part of ISO 9564 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 9564-1 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

This second edition cancels and replaces the first edition (ISO 9564-1:1991), which has been technically revised.

ISO 9564 consists of the following parts, under the general title *Banking — Personal Identification Number (PIN) management and security*:

— *Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

— *Part 2: Approved algorithm(s) for PIN encipherment*

— *Part 3: PIN protection requirements for offline PIN handling in ATM and POS systems*

Annexes A to G of this part of ISO 9564 are for information only.

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 or 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 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. As absolute security is not practically achievable, 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 the 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. The publication of additional parts is planned and these will cover PIN protection principles and techniques, electronic commerce and other environments identified at the time of writing.

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

ISO 9564-3:—[1)], *Banking — Personal Identification Number (PIN) management and security — Part 3: PIN protection requirements for offline PIN handling in ATM and POS systems*

ISO 10202 (all parts), *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards*

ISO 11568 (all parts), *Banking — Key management (retail)*

1) To be published.

ISO 13491 (all parts), *Banking — Secure cryptographic devices (retail)*

ISO 15668, *Banking — Secure file transfer (retail)*

Banking — Personal Identification Number (PIN) management and security —

Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems

1 Scope

This part of ISO 9564 specifies the basic principles and techniques which provide the minimum security measures required for effective international PIN management. These measures are applicable to those institutions responsible for implementing techniques for the management and protection of PINs.

This part of ISO 9564 also specifies PIN protection techniques applicable to financial transaction-card-originated transactions in an online environment and a standard means of interchanging PIN data. These techniques are applicable to those institutions responsible for implementing techniques for the management and protection of the PIN at Automated Teller Machines (ATM) and acquirer sponsored Point-of-Sale (POS) terminals.

The provisions of this part of ISO 9564 are not intended to cover:

a) PIN management and security in the offline PIN environment, which is covered in ISO 9564-3;

b) PIN management and security in the electronic commerce environments, which is to be covered in a subsequent part of ISO 9564;

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

d) privacy of non-PIN transaction data;

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

f) protection against replay of the PIN or transaction;

g) specific key management techniques.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 9564. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 9564 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

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

ISO 11568 (all parts), *Banking — Key management (retail)*

ISO 13491 (all parts), *Banking — Secure cryptographic devices (retail)*

ISO/IEC 7812 (all parts), *Identification cards — Identification of issuers*

ISO/IEC 7813:2001, *Identification cards — Financial transaction cards*

ISO/IEC 7816 (all parts), *Identification cards — Integrated circuit(s) cards with contacts*

3 Terms and definitions

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

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

3.2
algorithm
clearly specified mathematical process for computation

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

3.4
cipher text
data in its enciphered form

3.5
compromise
⟨cryptography⟩ breaching of secrecy and/or security

3.6
cryptographic key
mathematical value that is used in an algorithm to transform plain text into cipher text or vice versa

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

3.8
decipherment
reversal of a previous reversible encipherment rendering cipher text intelligible

3.9
dual control
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

EXAMPLE A cryptographic key is an example of the type of material to be accessed or utilized.

3.10
encipherment
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
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
exclusive OR-ing
binary addition with no carry

3.16
node
any message processing entity through which a transaction passes

3.17
notarization
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
code or password the customer possesses for verification of identity

3.19
PIN entry device
PED
device into which the cardholder inputs the PIN

NOTE A PIN entry device may also be called a PIN pad.

3.20
plain text
data in its original unenciphered form

3.21
primary account number
PAN
assigned number, composed of an issuer identification number, an individual account identification and an accompanying check digit, as specified in ISO/IEC 7812, that identifies the card issuer and card holder

3.22
pseudo-random number
number that is statistically random and essentially unpredictable although generated by an algorithmic process

3.23
reference PIN
value of the PIN used to verify the transaction PIN

3.24
reversible encipherment
transformation of plain text to cipher text in such a way that the original plain text can be recovered

3.25
split knowledge
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

3.26
terminal
acquirer-sponsored device that accepts ISO/IEC 7813 and/or ISO/IEC 7816 compliant cards and initiates transactions into a payments system

NOTE It may also include other components and interfaces such as host communications.

3.27
transaction PIN
PIN as entered by the customer at the time of the transaction

3.28
true random number generator
device that utilizes an unpredictable and non-deterministic physical phenomenon to produce a stream of bits, where the ability to predict any bit is no greater than 0,5 given knowledge of all preceding and following bits

3.29
variant of a key
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 of the PIN (as defined in 7.2) and until PIN deactivation (as defined in 7.8), 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 identified 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 6.3.2.

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 6.3.3.

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 G).

5 PIN entry devices

5.1 Character set

All PIN entry devices shall provide for the entry of the decimal numeric characters zero to nine.

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

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 entry device 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 6.3.2 for definition); however, the PIN entry device shall be secured as specified in 6.3.2 or 6.3.4.

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

When a remote PIN entry device 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 entry devices.

Table 2 — PIN entry device packaging consideration

	Terminal physically secure	**Terminal physically non-secure**
PIN entry device integral to terminal	Physical protection requirements as specified in 6.3.2 apply to the whole terminal. Terminal shall encipher PIN as specified in 6.2 for transmission.	Physical protection requirements as specified in 6.3.2 or 6.3.4 apply to PIN entry device. PIN entry device shall encipher PIN as specified in 6.2 for transmission.
PIN entry device remote to terminal	The PIN entry device shall be secured as specified in 6.3.2 or 6.3.4. PIN entry device shall encipher PIN as specified in 6.2 for transmission.	The PIN entry device shall be secured as specified in 6.3.2 or 6.3.4. PIN entry device shall encipher PIN as specified in 6.2 for transmission.

6 PIN security issues

6.1 PIN control requirements

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.

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 F).

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 entry devices 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 b)].

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.

PIN encipherment keys shall be at least 112 bits in length. A suitable technique is the use of a double-length DEA key as specified in ISO 11568-2.

ISO 11568-1 specifies general principles of key management.

6.3 Physical security

6.3.1 Physical security for PIN entry devices

This sub-clause defines a “physically secure device” and a “physically secure environment” and specifies requirements for a PIN entry device. Physical security requirements are specified in ISO 13491-1.

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 6.3.4 or the issuer's (or issuer's agent's) “physically secure environment”.

6.3.2 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 or manipulated to disclose all or part of any cryptographic key, PIN or other secret value 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 other secret values, and all useful residues of those 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).

6.3.3 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.

6.3.4 PIN entry device requirements

A PIN entry device shall comply with the requirements of 6.3.2 or, at a minimum, meet the following requirements:

a) Encipherment of a transaction PIN shall be implemented 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 either:

   — is unavailable for a sufficiently long time such that there is a high probability that its absence from its operational location is detected; and/or

   — 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 determination 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 See annex C 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 four and not more than twelve characters in length.

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 six digits in length. It is recommended, for security reasons, that a customer-selected alpha PIN should not be less than six characters in length. It should also be noted that many international systems do not accept more than six digits and/or do not support alpha PIN entry.

7.2 PIN selection

7.2.1 PIN selection techniques

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

a) assigned derived PIN;

b) assigned random PIN;

c) customer-selected PIN.

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

7.2.2 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.

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

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

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

7.2.3 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 D).

7.2.4 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 G for guidance).

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

7.3 PIN issuance and delivery

7.3.1 PIN issuance and delivery controls

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

The PIN shall never be retrieved and deciphered or regenerated for recording, processing, displaying, or printing 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.

7.3.2 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.

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.

NOTE 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.

7.3.3 Delivery of customer-selected PIN

7.3.3.1 PIN conveyance

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 7.3.3.2);

b) PIN selection by mail (see 7.3.3.3).

7.3.3.2 PIN selection at an issuer's location

PIN selection shall be accomplished at an issuer's location via a PIN entry device complying with the requirements of 5.4. 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.

7.3.3.3 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 ISO 11568. 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 7.3.2, 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 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

7.4.1 PIN change in an interchange environment

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.

7.4.2 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 7.3.3.2.

7.4.3 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.

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

7.4.4 PIN change by mail

The procedure for PIN change by mail shall be the same as specified for PIN selection in 7.3.3.3.

7.4.5 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 7.3.2 shall apply.

7.4.6 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 compromised 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.

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 or used some other means that:

— confirms PIN receipt; and

— confirms that this response is from the legitimate cardholder.

The receipt or response 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 the magnetic stripe of a card, it shall never be stored as plain text. If the PIN is to be stored on the magnetic stripe of a card, it shall be enciphered (e.g. PIN offset).

When the PIN (assigned or customer selected) is stored in the integrated circuit (IC) of a card, it should be stored within the protected area of the IC or it should be enciphered.

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 the customer's accounts associated with the PIN are closed.

c) The customer requests deactivation of the PIN.

d) The issuer otherwise determines that deactivation of the PIN is appropriate.

In the case of PIN compromise, or a deactivation request by the customer, 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 Examples of such measures are erasure of the deactivated PIN from the issuer's records and 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 entry device shall be the high-order digit (leftmost). The last digit to be entered shall be the low-order digit (rightmost).

Equipment used for interchange shall support entry of a four to twelve 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 and encipher 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

8.3.1 PIN block construction and format value assignment

This sub-clause 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 8.3.2
0001	:	Format 1, as defined in 8.3.3
0010	:	Format 2, as defined in ISO 9564-3
0011	:	Format 3, as defined in 8.3.5
0100 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

In international interchange, the format 0 PIN block or the format 3 PIN block should be used when the PAN is available, and the format 3 PIN block should be used when the same PIN encipherment key is used for multiple PIN encipherments.

8.3.2 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 8.3.2.1 and 8.3.2.2 respectively.

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

8.3.2.1 Plain text PIN field

The plain text PIN field shall be formatted as follows.

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F	

where

C = Control field: shall be binary 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).

8.3.2.2 Account number field

The account number field shall be formatted as follows.

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	

where

0 = Pad digit: a 4-bit field with the only permissible value of 0000 (zero);

A1 ... A12 = Account number: content is the 12 rightmost 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 zeros. Permissible values are 0000 (zero) to 1001 (9).

8.3.3 Format 1 PIN block

This PIN block is constructed by concatenation of two fields: the plain text PIN field and the transaction field.

The format 1 PIN block 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.

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
C	N	P	P	P	P	P/T	P/T	P/T	P/T	P/T	P/T	P/T	P/T	T	T	

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: designation of these fields is determined by the PIN length field;

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.

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.

8.3.4 Format 2 PIN block

The format 2 PIN block has been specified for local use with IC cards. The format 2 PIN block shall only be used in an offline environment and shall not be used for online PIN verification.

8.3.5 Format 3 PIN block

8.3.5.1 Format 3 PIN block construction

The format 3 PIN block is the same as format 0 PIN block except for the fill digits.

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 8.3.5.2 and 8.3.5.3 respectively.

The format 3 PIN block shall be reversibly enciphered when transmitted.

8.3.5.2 Plain text PIN field

The plain text PIN field shall be formatted as follows.

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F	

where

C = Control field: shall be binary 0011;

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, with values from 1010 (10) to 1111 (15), where the fill-digit values are randomly or sequentially selected from this set of six possible values, such that it is highly unlikely that the identical configuration of fill digits will be used more than once with the same account number field by the same PIN encipherment device.

8.3.5.3 Account number field

The account number field shall be formatted as follows.

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	

where

0 = Pad digit:	a 4-bit field with the only permissible value is 0000 (zero);
A1 ... A12 = Account number:	Content is the 12 rightmost 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 zeros. Permissible values are 0000 (zero) to 1001 (9).

8.4 Other PIN block formats

If the PIN block cannot be constructed in the terminal to comply with the formats 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 online PIN verification shall rest with the issuer, although the verification function may be delegated to another institution.

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

8.6 Journalizing of transactions containing PIN data

Terminals or other nodes in networks may be required to journalize (i.e. to record the full text of) transaction messages. Messages journalized shall not contain a plain text PIN. It is permissible to journalize 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.

A PIN should not be stored for longer than necessary.

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 ISO 11568-1 and as described in annex A.

Annex A
(informative)

General principles of key management

A.1 Cryptographic key hierarchy

Key management for this International Standard is specified in ISO 11568. This annex is for reference only.

Cryptographic keys may be hierarchically structured. Various environments may require different levels of hierarchy e.g. some terminals might require two levels. An example of a three-level hierarchy is as follows.

a) At the highest level of the hierarchy is the host master key. This key or 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).

A.2 Key generation for secret key algorithms

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

A.3 Protection against key disclosure

A cryptographic key only exists in the following forms:

a) as at least two key components controlled by the process of dual control and split knowledge. Each key component is generated as described in A.2. Each key component contains the same number of bits as the key itself;

   — the formation of a key from the key components depends 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 is 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 is ensured that the authorized employee who handles this component is the only person who has knowledge of its value and access to the component. There may be a nominated backup authorized employee who will only access the component in the case of the unavailability of the first authorized employee. These employees do not have access to another component that constitutes the same key;

b) in a device or system complying with the requirements of 6.3.2 or 6.3.4 or in an issuer's facility complying with 6.3.3;

c) in enciphered form, using a key enciphering key.

A.4 Protection against key substitution

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

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.

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 using 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 is deactivated and changed.

A.5 Restrictions on use of PIN protection keys

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

A.6 Limiting the effects of a key compromise

The following steps are taken 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 only exists at the minimum number of locations consistent with the effective operation of the system. This will, in many cases, be only two locations but where, for instance, resilient networks with alternative routing are used or hot-backup is employed, then these keys are, of necessity, held at more than two locations.

Any key used by a PIN entry device not complying with 6.3.2 is not 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 is, except by chance, 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 provides no information about any other cryptographic key.

The irreversible transformation of a key is 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.

A.7 Key replacement

A cryptographic key is replaced with a new key whenever the compromise of the original key is known or suspected. Knowledge of the original key does not provide any information which might be feasibly used to

determine the replacement key. The replacement key is not a variant of the original key, or an irreversible transformation of the original key.

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

Annex B
(informative)

PIN verification techniques

B.1 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;

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.

B.2 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 the PINs of those issuers.

B.3 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.

B.4 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 C
(informative)

PIN entry device for online PIN encipherment

C.1 General

This part of ISO 9564 (see 6.3.4) 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 in accordance with this International Standard, 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 where 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 has to be able to determine the current key in each of many (perhaps tens of thousands) PIN entry devices There are a number of techniques by which this can be achieved. Three techniques are described in C.2 to C.4.

C.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 enciphering 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 transforming the current key to generate a new key.

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

This approach operates essentially as described in C.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 and is consequently available to the acquirer's physically secure device when it processes this transaction. Attention is drawn to the fact 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 ensures 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 has to 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.

C.4 Derived unique key per transaction

This technique is similar to the technique described in C.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 online 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 one million unique keys, the acquirer's can compute the current key in no more than 12 encipherment operations.

Annex D
(informative)

Example of pseudo-random PIN generation

This example uses the Data Encryption Algorithm, ANSI X3:92:1993. 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 is to 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.

Warning, this technique yields digits with a negligible bias towards the digits 0 to 5, this bias is negligible only for PIN-length from four to six characters.