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.