INTERNATIONAL STANDARD

ISO 9564-1

First edition
1991-12-15

Banking — Personal Identification Number management and security —

Part 1:
PIN protection principles and techniques

Banque — Gestion et sécurité du numéro personnel d'identification —

Partie 1: Principes et techniques de protection du PIN

Reference number
ISO 9564-1:1991(E)

Contents

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Annexes

Foreword

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

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

International Standard ISO 9564-1 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Sub-Committee SC 6, *Financial transaction cards, related media and operations*.

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

— *Part 1: PIN protection principles and techniques*

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

Annexes A and B form an integral part of this part of ISO 9564. Annexes C, D, E, F, G and H 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 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.

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 it 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-