INTERNATIONAL STANDARD

ISO 9564-1

Third edition
2011-02-15

Financial services — Personal Identification Number (PIN) management and security —

Part 1: Basic principles and requirements for PINs in card-based systems

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

Partie 1: Principes de base et exigences relatifs aux PINs dans les systèmes à carte

Reference number
ISO 9564-1:2011(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.org
Web www.iso.org

Published 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 2.

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 document 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, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This third edition cancels and replaces the second edition (ISO 9564-1:2002) and the first edition of ISO 9564-3:2003, which have been technically revised.

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

— *Part 1: Basic principles and requirements for PINS in card-based systems*

— *Part 2: Approved algorithm(s) for PIN encipherment*[1)]

— *Part 3: Requirements for offline PIN handling in ATM and POS systems* [Withdrawn and incorporated into Part 1]

— *Part 4: Guidelines for PIN handling in open networks* [Technical Report][1)]

1) It is intended that, upon revision, the main element of the titles of Parts 2 and 4 will be aligned with the main element of the title of this part of ISO 9564.

Introduction

A Personal Identification Number (PIN) is used in financial services as one method of cardholder verification.

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 electronic funds transfer (EFT) systems. The secrecy of the PIN needs to be assured at all times during its life cycle, which consists of its establishment, issuance, activation, storage, entry, transmission, validation, deactivation and any other use made of it.

In this part of ISO 9564, the following terms are used for the types of communication of the PIN:

a) conveyance: reference PIN to the integrated circuit (IC) card or cardholder selected PIN to the issuer;

b) delivery: PIN to the cardholder;

c) transmission: transaction PIN to the issuer or IC reader for subsequent PIN verification;

d) submission: transaction PIN to the IC card.

PIN security in part 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.

PINs can be verified online or offline. Since online PIN verification can be performed independent of the card itself, any type of payment card or device can be used to initiate such a transaction. However, there are special card requirements for those cards that perform offline PIN verification on the card itself.

Financial transaction cards with embedded IC can support offline PIN verification using the IC of the card. Issuers can choose whether to have PIN verification performed online or offline. Offline PIN verification does not require that a cardholder's PIN be sent to the issuer host for verification and so security requirements relating to PIN protection differ from online PIN verification security requirements. However, many general PIN protection principles and techniques are still applicable even though a PIN can be verified offline.

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.

In ISO 9564-2, approved encipherment algorithms for use in the protection of the PIN are specified. Application of the requirements of this part of ISO 9564 requires the making of bilateral agreements, including the choice of algorithms specified in ISO 9564-2.

ISO 9564 (all parts) is one of several series of International Standards which describe requirements for security in the retail banking environment; these include ISO 11568 (all parts), ISO 13491 (all parts) and ISO 16609.

Additionally, it is intended to develop an extended PIN block in order to support the use of block ciphers with longer block lengths and key sizes (e.g. AES).

Financial services — Personal Identification Number (PIN) management and security —

Part 1: Basic principles and requirements for PINs in card-based 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 during their creation, issuance, usage and deactivation.

This part of ISO 9564 is applicable to the management of cardholder PINs for use as a means of cardholder verification in retail banking systems in, notably, automated teller machine (ATM) systems, point-of-sale (POS) terminals, automated fuel dispensers, vending machines, banking kiosks and PIN selection/change systems. It is applicable to issuer and interchange environments.

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

a) PIN management and security in environments where no persistent cryptographic relationship exists between the transaction-origination device and the acquirer, e.g. use of a browser for online shopping (for these environments, see ISO/TR 9564-4);

b) protection of the PIN against loss or intentional misuse by the customer;

c) privacy of non-PIN transaction data;

d) protection of transaction messages against alteration or substitution;

e) protection against replay of the PIN or transaction;

f) specific key management techniques;

g) offline PIN verification used in contactless devices;

h) requirements specifically associated with PIN management as it relates to multi-application functionality in IC cards.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

ISO/IEC 7813, *Information technology — Identification cards — Financial transaction cards*

ISO/IEC 7816-1, *Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics*

ISO/IEC 7816-2, *Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts*

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 7816-4, *Identification cards — Integrated circuit cards – Part 4: Organization, security and commands for interchange*

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

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

ISO 13491-1:2007, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ISO 13491-2:2005, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

3 Terms and definitions

For the purposes of this document, 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
cardholder PIN
PIN known by the cardholder

3.5
cipher text
data in their enciphered form

3.6
compromise
⟨cryptography⟩ breaching of confidentiality and/or integrity

3.7
cryptographic key
mathematical value that is used in an algorithm to transform plain text into cipher text or vice versa

3.8
customer
cardholder
individual associated with the primary account number (PAN) specified in the transaction

3.9
decipherment
reversal of a previous reversible encipherment rendering cipher text into plain text

3.10
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 protected by dual control.

3.11
encipherment
rendering of text unintelligible by means of an encoding mechanism

3.12
integrated circuit
IC
microprocessor (typically) embedded in an IC card as specified in ISO/IEC 7816 (all parts)

3.13
IC card
ICC
integrated circuit card as specified in ISO/IEC 7816 (all parts)

NOTE All references to an IC card are understood to be references to the IC of the card and not to any other storage on the card (e.g. magnetic stripe).

3.14
irreversible encipherment
transformation of plain text to cipher text in such a way that the original plain text cannot be recovered other than by exhaustive procedures, even if the cryptographic key is known

3.15
issuer
institution holding the account identified by the primary account number (PAN)

3.16
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

3.17
modulo-2 addition
exclusive OR-ing
binary addition with no carry

3.18
node
any message processing entity through which a transaction passes

3.19
Personal Identification Number
PIN
string of numeric digits established as a shared secret between the cardholder and the issuer, for subsequent use to validate authorized card usage

3.20
PIN entry device
PED
device providing for the secure entry of PINs

NOTE Security requirements for PIN entry devices are specified in 5.1.

3.21
plain text
data in its original unenciphered form

3.22
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 7812-1, which identifies the card issuer and cardholder

3.23
pseudo-random number
number that is statistically random and essentially unpredictable although generated by an algorithmic process

3.24
reference PIN
value of the PIN used to verify the transaction PIN

3.25
reversible encipherment
transformation of plain text to cipher text in such a way that the original plain text can be recovered

3.26
sensitive state
device condition that provides access to the secure operator interface such that it can only be entered when the device is under dual or multiple control

3.27
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

3.28
terminal
acquirer-sponsored device that accepts ISO/IEC 7813 and ISO/IEC 7816 compliant cards and initiates transactions into a payments system

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

3.29
transaction PIN
PIN as entered by the customer at the time of the transaction and subsequently transmitted to an issuer system or submitted to the IC card for verification

NOTE Verification means comparison to the reference PIN.

3.30
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

4 Basic principles of PIN management

4.1 General

The term “PIN” is used to describe any string of numeric digits established as a shared secret between the cardholder and the issuer, for subsequent use to validate authorized card usage. The term PIN may be qualified as “cardholder PIN”, “reference PIN” and “transaction PIN” in the following ways.

a) Issuance:

   1) the PIN

      i) is generated by the issuer and delivered to the cardholder (as the cardholder PIN), or

      ii) is selected by the cardholder and conveyed to the issuer;

   2) the issuer stores the PIN as the reference PIN or stores data such that the reference PIN can be recalculated; the reference PIN may be stored in the issuer system and/or an IC card.

b) Usage:

   1) the cardholder enters their PIN into a PED. The PIN, once entered into a PED, is the transaction PIN;

   2) the transaction PIN is transmitted to the issuer or sent to the IC card for comparison with the reference PIN.

Some requirements pertain to all PINs while other requirements are specific to cardholder PINs, reference PINs, and/or transaction PINs. Where requirements apply to all PINs, the term PIN is used without qualification.

4.2 Principles

PIN management shall be governed by the following basic principles.

a) Fraudulent modification or access to the hardware and software used for all PIN management functions shall be prevented or detected (see 6.1.1).

b) For different accounts, encipherment of the same PIN value under a given encipherment key shall not predictably produce the same cipher text (see 6.2).

c) Security of an enciphered PIN shall not rely on the secrecy of the encipherment design or algorithm, but on the security of the cryptographic key (see 6.2).

d) A PIN shall not exist outside of a secure cryptographic device, as defined in 5.1, except in the following cases:

   1) delivery of the PIN to the cardholder using an approved method as defined in 8.3;

   2) enciphered using an approved algorithm, as defined in 6.2, in a process that ensures two accounts with the same PIN do not have the same encrypted value; this process may use PIN block formats 0 or 3;

   3) conveyance of the reference PIN to the IC card to enable offline PIN verification, as defined in 8.9;

   4) storage of a reference PIN within an IC card in accordance with 7.3;

   5) submission of a transaction PIN to an IC card in accordance with 9.2.2.

e) PIN issuance shall be performed only by personnel authorized by the issuer, as defined in 8.3.

f) PIN selection/change shall be performed only by the cardholder, as defined in 8.2.4 and 8.5.

g) Management of PIN establishment/change devices shall be performed only by personnel authorized by the issuer, except as allowed in 8.5. Such personnel shall operate only under strictly enforced procedures.

h) With the exception of PIN selection/change by mail (see 8.4.4 and 8.5.5), the PIN shall never be known to, or accessible by, any employee or agent of the institution, not even in the PIN issuing process.

i) A stored reference PIN shall be protected from unauthorized substitution, as defined in 8.9.

j) Compromise of the PIN (or suspected compromise) shall result in the ending of the PIN life cycle, as defined in 8.10.

k) Responsibility for PIN verification shall rest with the issuer, as defined in 7.2 and 7.3.

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

m) The customer shall be advised in writing of the importance of the PIN and PIN secrecy (see Annex C for guidance).

n) Cleartext and/or enciphered transaction PINs shall never be retained. Transaction PINs shall only exist for the duration of a single transaction (the time between PIN entry and verification, i.e. store and forward).

For the purposes of this part of ISO 9564, an IC card is considered to be part of the issuer's domain.

5 PIN handling devices

5.1 PIN handling device security requirements

A PIN handling device is a device that handles clear text PINs, e.g. PIN entry device, IC reader and host security module, etc. Any additional functionality provided by the device or the system into which it is integrated shall not impair the security of the device or the PIN entry process. A PIN handling device, other than an IC card, shall be a secure cryptographic device specifically meeting the requirements of ISO 13491-1:2007, 6.2.5 and 6.3, i.e. a physically secure device. The security requirements for IC cards are specified in 7.3.

A PIN entry device shall not rely on tamper evidence as its sole physical security characteristic.

The PIN entry device shall include tamper-detection and response mechanisms which, if attacked, cause the PED to become immediately inoperable and result in the automatic and immediate erasure of any secret information that might be stored in the PED, such that it becomes infeasible to recover the secret information.

The PIN entry device should be able to authenticate itself to the acquirer such that, once compromised, it is no longer able to authenticate itself to the acquirer. An example method to support this requirement is where Message Authentication Codes (MAC) are calculated over online transaction messages and the MAC key is erased if the PIN entry device is attacked.

NOTE Systems supporting online PIN verification typically meet this requirement in that the acquirer authenticates the validity of the PIN entry device each time a PIN is processed. (The authentication of the PIN entry device is implicit in the usage of the PIN encryption key.)

The display used to prompt a cardholder to enter their PIN shall be controlled such that modification and/or improper use of the prompts is not feasible (see ISO 13491-2:2005, B.2.1, number B2, and B.2.2, number B16).

The card reader shall be protected to prevent unauthorized access, substitution or alteration of the card data read from the card (see ISO 13491-2:2005, B.2.1, number B3, and B.2.2, number B22).