
**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*



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

STANDARDSISO.COM : Click to view the full PDF of ISO 9564-1:2011



COPYRIGHT PROTECTED DOCUMENT

© ISO 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Basic principles of PIN management	5
4.1 General	5
4.2 Principles	5
5 PIN handling devices	6
5.1 PIN handling device security requirements	6
5.2 Physical security for IC readers.....	7
5.3 PIN entry device characteristics	7
6 PIN security issues.....	7
6.1 PIN control requirements.....	7
6.2 PIN encipherment	8
7 PIN verification	9
7.1 General	9
7.2 Online PIN verification	9
7.3 Offline PIN verification	9
8 Techniques for management/protection of account-related PIN functions	9
8.1 PIN length	9
8.2 PIN establishment	9
8.3 PIN issuance and delivery to the cardholder	10
8.4 PIN selection	10
8.5 PIN change	11
8.6 PIN replacement	12
8.7 Disposal of waste material and returned PIN mailers	12
8.8 PIN activation.....	13
8.9 PIN storage.....	13
8.10 PIN deactivation.....	13
8.11 PIN mailers	14
9 Techniques for management/protection of transaction-related PIN functions	14
9.1 PIN entry	14
9.2 Protection of PIN during transmission.....	14
9.3 Compact PIN block formats	17
9.4 Extended PIN blocks	22
9.5 Journalizing of transactions containing PIN data.....	22
10 Approval procedure for encipherment algorithms	22
Annex A (normative) Destruction of sensitive data	23
Annex B (informative) Additional guidelines for the design of a PIN entry device.....	25
Annex C (informative) Information for customers	28
Bibliography.....	29

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 encipherment¹⁾*
- *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).

STANDARDSISO.COM : Click to view the full PDF of ISO 9564-1:2017

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).

5.2 Physical security for IC readers

The following requirements are specific to IC readers. The slot of the IC reader into which the IC card is inserted should

- a) not have sufficient space to hold a PIN-disclosing “bug” when a card is in the IC reader,
- b) nor be enlarged to provide space for a PIN-disclosing “bug” without detection,
- c) nor be positioned such that wires leaving the slot to an external “bug” can be hidden from users of the device.

5.3 PIN entry device characteristics

5.3.1 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, can 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 B.

5.3.2 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

6 PIN security issues

6.1 PIN control requirements

6.1.1 PIN processing systems

PIN processing systems are systems that process PINs in all stages of the PIN life cycle, e.g. merchant terminal systems, host application software driving host security modules, and card and PIN personalization systems, etc.

Systems used in PIN processing shall be implemented in such a way that the following are assured.

- a) The hardware and software are correctly performing their designed function and only their 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 is not capable of being used or misused to determine a PIN by exhaustive trial and error.
- e) Any PIN management device (e.g. host security modules) handling clear text PINs conforms to the requirements of Secure Cryptographic Devices with PIN management functionality, as specified in ISO 13491-2:2005, Annex C.
- f) Output of any sensitive information used in the selection, calculation or encipherment of the PIN is controlled during use, delivery, conveyance, submission, transmission, storage and disposal.
- g) Except when the PIN is to be sent to the IC card in clear text, the PIN is enciphered immediately upon entry into the PED.

6.1.2 Recording media

Any recording media containing data from which a plain text PIN might be determined shall be rendered unreadable or physically destroyed immediately after use (see Annex A).

6.1.3 Oral communications

No procedure shall require or permit oral communication of the plain text PIN, either in person or by a person over the telephone.

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 at any time in the PIN life cycle, unless the telephone device is designed and constructed to meet the requirements specified in 5.1 for PIN entry devices and 9.2 for PIN transmission.

6.2 PIN encipherment

If it is necessary to encipher a PIN (see 9.2), this shall be accomplished using one of the approved algorithms specified in ISO 9564-2.

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

Symmetric PIN encipherment keys may be used in online and offline PIN verification systems. Symmetric PIN encipherment keys shall not be used for any other cryptographic purpose.

Asymmetric PIN encipherment is only permitted in offline PIN verification systems. Asymmetric PIN encipherment keys should not be used for any other cryptographic purpose.

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.

NOTE A format 2 PIN block does not meet this requirement without additional protection mechanisms.

Key management practices associated with PIN encipherment shall comply with the requirements of ISO 11568 (all parts).

7 PIN verification

7.1 General

PIN verification is the process whereby a transaction PIN is compared to a reference PIN to determine whether the two have the same value. Derivatives of the transaction and reference PINs may be used during the PIN verification process in lieu of the clear text PIN.

7.2 Online PIN verification

Transaction PINs are verified online after secure transmission to the issuer according to 9.2.1. Responsibility for online PIN verification shall rest with the issuer.

7.3 Offline PIN verification

Transaction PINs are verified offline after submission to the IC card according to 9.2.2. Responsibility for offline PIN verification shall rest with the issuer through programming/configuration of the IC card which is under issuer control.

An ICC containing a reference PIN for offline PIN verification shall provide a level of protection against known attacks on the ICC sufficient to prevent recovery of the plain text reference or transaction PIN or any other secrets stored within the ICC.

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

8.1 PIN length

A PIN shall be not less than four and not more than 12 digits 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.

8.2 PIN establishment

8.2.1 PIN establishment techniques

A PIN shall be established using one of the following techniques:

- a) assigned derived PIN;
- b) assigned random PIN;
- c) customer-selected PIN.

It is recommended that, regardless of the method used to establish a PIN, PIN values be checked against known weaknesses as described in Annex C.

8.2.2 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.

8.2.3 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.

These may be achieved using a random number generator compliant with ISO/IEC 18031 and tested using NIST SP 800-22.

8.2.4 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 C for guidance).

8.3 PIN issuance and delivery to the cardholder

Methods used for the issuance and delivery of the PIN to the cardholder shall comply with the following basic requirements.

- a) The plain text PIN shall never be transmitted over communications lines outside of a secure environment as specified in ISO 13491-2:2005, H.4, number H5, unless there is no feasible way in which the PIN could be related to the cardholder, the cardholder's account or card.
- b) The PIN shall never be known to, or accessible by, any employee or agent of the institution, not even in the PIN issuing process.
- c) All PIN issuance functions involving issuer personnel (including their agents) shall be under dual control.
- d) At no point in the delivery process shall the PIN appear in plain text where it can be associated with a customer's account or primary account number (PAN).
- e) The PIN shall never be retrieved and deciphered or regenerated for recording, processing, displaying or printing, except for presentation to the cardholder in a manner that ensures the secrecy of the PIN (e.g. a PIN mailer implemented in accordance with 8.11 or personal secure cryptographic device with display capability).
- f) Where it is necessary, for the purposes of preparing the PIN for delivery to the cardholder, for the PIN to exist as plain text outside of a secure cryptographic device (e.g. PIN mailer printing), then it shall exist in that condition for the minimum period of time necessary and it shall be contained within a secure environment, as specified in ISO 13491-2:2005, H.5.

8.4 PIN selection

8.4.1 General

PIN selection is a process performed by the cardholder either as part of the card issuance process or during PIN change.

8.4.2 PIN conveyance

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

- a) PIN selection at an issuer's location (see 8.4.3);
- b) PIN selection by mail (see 8.4.4).

8.4.3 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 5.1. 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.
- e) The entry of the PIN shall be validated by requiring it to be entered twice and verifying that both entries are identical. The comparison of the two PIN entries shall be performed in a manner such that no PIN information is exposed.

8.4.4 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 (all parts). 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 8.11, 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.

The control number may be the reversibly enciphered account number.

8.5 PIN change

8.5.1 General

PIN change is a request initiated by the cardholder. It is a process including a PIN selection followed by the update of PIN-related data, where necessary (e.g. on the card and in host systems, etc.). PIN change shall be performed in accordance with the requirements of 8.4.

8.5.2 PIN change in an interchange environment

When implemented in an interchange environment, PIN change shall be performed only for IC cards and then only where the updating of the PIN in the IC card is performed through a cryptographically controlled relationship between the issuer and the IC card.

8.5.3 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 8.4.3.

8.5.4 PIN change at an unattended terminal

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

The entry of the new PIN shall be validated by requiring it to be entered twice and verifying that both entries are identical. The comparison of the two PIN entries shall be performed in a manner such that no PIN information is exposed.

8.5.5 PIN change by mail

The card issuer shall authenticate the cardholder prior to dispatching the PIN change form. The issuer should communicate with the cardholder, notifying them of means of dispatch. Such communications should be performed using the method of record.

The remaining procedure for PIN change by mail shall be the same as specified for PIN selection in 8.4.4.

NOTE This process is not suitable for applications where PIN related data needs to be updated on the card.

8.6 PIN replacement

8.6.1 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 issuer shall authenticate the cardholder prior to issuing a replacement PIN. The procedures used to replace a forgotten PIN shall follow those covered in 8.3.

8.6.2 Re-advice of forgotten PIN

Re-advice of a forgotten PIN shall be performed through the issuer's system; it shall not be performed in an interchange environment. The issuer shall authenticate the cardholder prior to re-advising the cardholder of their forgotten PIN. The procedures used to re-advice a customer of their forgotten PIN shall follow those covered in 8.3.

8.6.3 Replacement of compromised PIN

When a PIN is believed to have been compromised it shall be deactivated as soon as possible (see 8.10) 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 8.8).

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.

8.7 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 printing of PIN mailers.

Return addresses for card and PIN mailers should be different.

8.8 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.

8.9 PIN storage

PIN storage shall be implemented in accordance with the requirements of 4.2 d).

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.

A plain text PIN shall never be stored on the magnetic stripe of a card.

If values related to the PIN are stored (e.g. PIN offset), it shall not be possible to reconstruct the PIN without knowledge of the cryptographic keys used to generate the values.

Unauthorized substitution of the reference PIN shall be prevented. For example the reference PIN may be cryptographically bound to the associated account/card number.

When the reference PIN is stored in the IC card for subsequent offline PIN verification, it shall be protected in accordance with 7.3.

The conveyance of a clear text reference PIN to the IC card shall be performed solely within a secure environment conforming to the requirements of ISO 13491-2:2005, H.5.

8.10 PIN deactivation

PIN deactivation is where a cardholder's PIN (and typically the card associated with that PIN) is invalidated within the issuer system, such that it can no longer be used to perform transactions. In the case of an IC card, PIN deactivation means blocking the PIN, account or card, as appropriate. This should not be confused with PIN suspension where a PIN is made temporarily unusable for transactions, e.g. due to exceeding the maximum number of consecutive failed PIN tries.

Responsibility for PIN deactivation rests with the issuer. An issuer shall deactivate a PIN at the first possible opportunity 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 card associated with 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 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.

8.11 PIN mailers

A PIN mailer may consist of an outer layer, e.g. envelope and an inner tamper-evident portion used to protect the PIN. These two elements may be combined as a single tamper-evident PIN mailer.

The following requirements apply where PIN mailers are used to deliver an assigned PIN to the cardholder.

- a) The PIN mailer shall be tamper evident, such that it is infeasible for the plain text PIN to be determined fraudulently or accidentally, without such access being obvious to the cardholder.
- b) The externally visible portions of the PIN mailer shall display the minimum data necessary to deliver the PIN mailer to the correct cardholder.
- c) The issuer shall warn the cardholder not to use a PIN that is contained in an opened or tampered PIN mailer and to notify the issuer of such an event.
- d) The PIN mailer shall not contain sufficient information to allow anyone other than the cardholder to determine the account number associated with the PIN. For instance, the last four digits of the account number may be included in the private portion of the PIN mailer.

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

- e) The PIN and card shall neither be mailed in the same mailer nor at the same time, to minimize the probability of simultaneous receipt.
- f) The PIN mailer should be delivered without other materials that might lead to the PIN mailer being discarded without being noticed.

Additionally the issuer should notify the cardholder of the despatch of the PIN mailer using the communications method of record.

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 or keep the mailer in a safe place.

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

9.1 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 4- to 12-digit PIN.

9.2 Protection of PIN during transmission

9.2.1 PIN protection during transmission to the issuer for online PIN verification

During transmission through a network, including within network nodes, a PIN shall be protected by one or both of the following means:

- a) provision of physical protection (see 5.1);
- 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.

9.2.2 PIN protection during conveyance to the ICC for offline PIN verification

9.2.2.1 Configuration

The IC reader and PIN entry device can either be integrated into a single device or be two separate devices.

- a) When the IC reader and PIN entry device are integrated within a device meeting the requirements of 5.1,
 - 1) if the PIN is to be submitted to the IC card in plain text form, the device need not encipher the PIN; it simply submits the PIN to the IC card, or
 - 2) if the PIN is to be submitted to the IC card in enciphered form, then the device shall encipher the PIN using the authenticated encipherment key of the IC card and submit the enciphered PIN to the IC card.
- b) If the PIN is to be submitted to the IC reader through an unprotected environment, i.e. the PIN entry device and the IC reader are not integrated within a device meeting the requirements of 5.1, the PIN shall be enciphered by the PIN entry device in accordance with 6.2. The enciphered PIN shall then be submitted to the IC reader and the IC reader shall then
 - 1) decipher the PIN for submission in plain text to the IC card,
 - 2) decipher the PIN and then re-encipher it using the authenticated encipherment key of the IC card and submit the enciphered PIN to the IC card, or
 - 3) submit the enciphered PIN to the IC card (if the PIN is already enciphered using the authenticated encipherment key of the IC card).

All PIN encipherment operations shall occur within a device meeting the requirements of 5.1.

If the PIN is to be submitted to the IC card in enciphered form, the integrity and authenticity of the PIN encipherment key of the IC card shall be ensured by

- protecting against substitution of the encipherment key during its handling within the IC reader and PED, e.g. by using an integrity-ensured channel between the IC reader and the PED, and
- verifying that the encipherment key is chained to a trusted public key installed in the device performing the authentication.

Table 2 summarizes the PIN protection requirements for various terminal configurations and PIN submission methods as detailed above in this subclause.

Table 2 — ICC PIN protection summary

PIN submission method	PIN entry device and IC reader integrated [see 9.2.2.1 a)]	PIN entry device and IC reader not integrated [see 9.2.2.1 b)]
Plain text PIN submitted to the IC card	No encipherment is required. The plain text PIN is submitted to the IC card [see 9.2.2.1 a) 1)].	The PIN is enciphered from the PIN entry device to the IC reader in accordance with 6.2. The plain text PIN is then decrypted and submitted to the IC card [see 9.2.2.1 b) 1)].
Enciphered PIN submitted to the IC card	The PIN is submitted to the IC card enciphered using an authenticated encipherment key of the IC card [see 9.2.2.1 a) 2)].	The PIN is enciphered (using a symmetric key) by the PIN entry device in accordance with 6.2. The IC reader receives the enciphered PIN, deciphers the PIN and then re-enciphers it using the authenticated encipherment key of the IC card. The enciphered PIN is then submitted to the IC card [see 9.2.2.1 b) 2)]. or The PIN is enciphered (using the authenticated encipherment key of the IC card) by the PIN entry device in accordance with 6.2. The IC reader receives the enciphered PIN and then submits it to the IC card [see 9.2.2.1 b) 3)].

9.2.2.2 PIN block format

The PIN that is submitted by the IC reader to the IC shall be contained in a PIN block conforming to the format 2 PIN block requirements of 9.3.4. This applies whether the PIN is submitted in plaintext or enciphered using an encipherment key of the IC.

PINs enciphered only for transmission between the PIN entry device and the IC reader shall use one of the PIN block formats specified in 9.3 or 9.4. Where format 2 PIN blocks are used, a unique key per transaction method in accordance with ISO 11568 (all parts) shall be used.

9.2.2.3 Encryption block format

When a PIN is to be presented encrypted to the IC, the format 2 PIN block shall be formatted within an encryption block as shown in Figure 1. The encryption block is then encrypted using the authenticated encipherment key of the IC. The process is fully described in EMV Book 2.

Field name	Length	Description
Data Header	1	Hex value "7F".
PIN Block (format 2)	8	PIN in PIN block (see 9.3.4).
ICC Unpredictable Number	8	Unpredictable number obtained from the ICC.
Random Pad	$N_{IC} - 17$	Random pad generated by the terminal.

NOTE N_{IC} is the length in bytes of the authenticated encipherment key of the IC.

Figure 1 — ICC encryption block format

The value of the random pad shall be unpredictable (even given knowledge of previous values) and prior to encipherment shall only exist in hardware suitable for protecting the plain text PIN. For each encryption, all values should be equally likely to be generated (e.g. there is no internal structure or repetition).

This may be achieved using a random number generator compliant with ISO/IEC 18031 and tested using NIST SP 800-22.

9.3 Compact PIN block formats

9.3.1 PIN block construction and format value assignment

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

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

0000	:	Format 0, as defined in 9.3.2
0001	:	Format 1, as defined in 9.3.3
0010	:	Format 2, as defined in 9.3.4
0011	:	Format 3, as defined in 9.3.5
0100 through 0111	:	For allocation by Technical Committee 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 shall be used when the PAN is available. The format 3 PIN block should be used when the same PIN encipherment key is used for multiple PIN encipherments (e.g. fixed or session key management).

9.3.2 Format 0 PIN block

9.3.2.1 General

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 9.3.2.2 and 9.3.2.3, respectively.

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

9.3.2.2 Plain text PIN field

The plain text PIN field shall be formatted in the following way.

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	F	F								
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	-----	---	---

where

C = Control field:	4-bit field value 0000 (zero);
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).

9.3.2.3 Account number field

The account number field shall be formatted in the following way.

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).

9.3.3 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 in the following way.

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	T	T							
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	---	---

where

- C = Control field: 4-bit field value 0001 (1);
- 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.

9.3.4 Format 2 PIN block

The format 2 PIN block has been specified for 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. This PIN block is constructed by concatenation of two fields: the plain text PIN field and the filler field.

The format 2 PIN block shall be formatted in the following way:

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	F	F							
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	---	---

where

- C = Control field: 4-bit field value 0010 (2);
- 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/F = PIN/Fill digit: designation of these fields is determined by the PIN length field;
- F = Fill digit: 4-bit field value 1111 (15).

A format 2 PIN block shall be formatted within an encryption block when enciphered by the authenticated encipherment key of the IC (see 9.2.2.3).

9.3.5 Format 3 PIN block

9.3.5.1 Format 3 PIN block construction

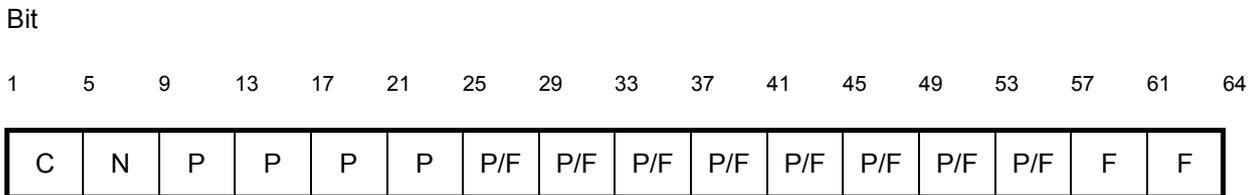
The format 3 PIN block is the same as format 0 PIN block except for the fill digits.

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 9.3.5.2 and 9.3.5.3 respectively.

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

9.3.5.2 Plain text PIN field

The plain text PIN field shall be formatted in the following way.

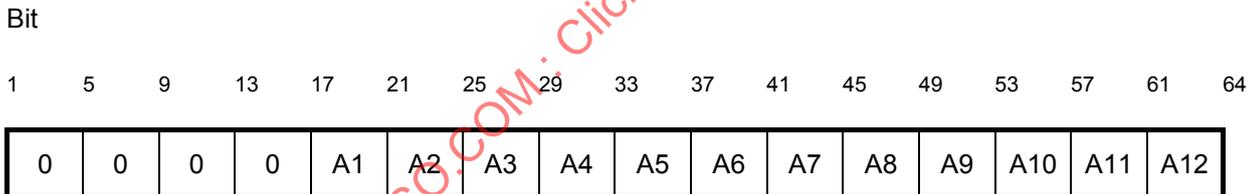


where

- C = Control field: 4-bit field value 0011 (3);
- 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 is used more than once with the same account number field by the same PIN encipherment device.

9.3.5.3 Account number field

The account number field shall be formatted in the following way.



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).

9.3.6 Compact PIN block usage restrictions

To ensure PIN security, the following restrictions shall apply to usage of compact PIN blocks.

- a) Controls shall be in place to prevent the misuse of card issuance-related functions (including PIN change).
- b) Standard PIN block formats (e.g. ISO format 0, 1, 2 and 3) shall not be translated into non-standard PIN block formats.
- c) Use of format 2 PIN blocks shall be constrained to offline PIN verification and PIN change operations in ICC environments only.
- d) Translation of PIN block formats that include the PAN to PIN block formats that do not include the PAN, shall not be supported. In particular, ISO PIN block formats 0 and 3 shall not be translated into ISO PIN block format 1.
- e) When performing translations between PIN block formats that both include the PAN, a change of PAN shall not be supported except in the following case: where introduction of a new PAN is required to support account number changes for card issuance, support for change of PAN shall only be provided whilst the host security modules are in a sensitive state and under dual control (see ISO 13491-1:2007, 6.3.6) and shall not be performed in interchange processing systems.
- f) Only ISO formats 0 and 3 shall be supported in calculating values used for PIN verification that are derived from the PIN and PAN, e.g. PIN offsets and PIN verification values (PVV).
- g) When calculating values derived from the PIN and PAN, if the portion of the account number enciphered in the input encrypted PIN block does not agree with the input PAN, the calculated value shall not be returned except in the following case: where the introduction of a new PAN is required to support account number changes for card issuance, support for change of PAN during calculation of the derived value shall be provided only whilst the host security modules are in a sensitive state and under dual control (see ISO 13491-1:2007, 6.3.6).
- h) Any integrity checks performed on the deciphered PIN block shall rely only on the first byte of the PIN block (control field and PIN length field) and fill digits (to ensure that each digit is a permitted value).

Table 3 illustrates requirements c), d) and f) for translations from formats 0, 1 and 3.

Table 3 — Requirements for translations

Translation from	Translation to			
	ISO format 0	ISO format 1	ISO format 2	ISO format 3
ISO format 0	Permitted anywhere without change of PAN Change of PAN only permitted in sensitive state for card issuance	Not permitted	Permitted for submission to an IC card	Permitted anywhere without change of PAN Change of PAN only permitted in sensitive state for card issuance
ISO format 1	Permitted	Permitted	Permitted for submission to an IC card	Permitted
ISO format 2	Not permitted	Not permitted	Permitted for submission to an IC card	Not permitted
ISO format 3	Permitted anywhere without change of PAN Change of PAN only permitted in sensitive state for card issuance	Not permitted	Permitted for submission to an IC card	Permitted anywhere without change of PAN Change of PAN only permitted in sensitive state for card issuance

9.4 Extended PIN blocks

When the PIN is to be enciphered using a 128-bit or greater block cipher (e.g. AES), it shall be formatted using an extended PIN block approved by Technical Committee ISO/TC 68, Subcommittee SC 2.

NOTE 1 It is intended to develop an extended PIN block (see Introduction).

NOTE 2 Support for block ciphers with longer block and key lengths does not imply phasing out of block ciphers currently in use, such as TDEA.

9.5 Journalizing of transactions containing PIN data

Messages journalized (post-authorization storage) shall not contain plain text or enciphered PINs in any form.

10 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 11568-1:2005, Annex A.