INTERNATIONAL STANDARD

ISO 9564-1

Third edition
2011-02-15

AMENDMENT 1
2015-03-01

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

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

AMENDMENT 1

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

AMENDEMENT 1

Reference number
ISO 9564-1:2011/Amd.1:2015(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

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 68, *Financial Services*, Subcommittee SC 2, *Security*.

Introduction

Although TDEA is still considered secure for PIN encryption and there are no current plans to migrate away from TDEA, experience shows that migration to a new PIN encipherment algorithm for the financial industry can require a very long time. At the same time, there are regional regulatory efforts underway to introduce AES as an eventual replacement for TDEA. In order to facilitate early adopters and vendors, it is desirable to establish early on a PIN block format that will ensure long-term interoperability when using block ciphers with a larger block size than TDEA.

It must be emphasized that no short or medium term move away from TDEA as an approved algorithm for PIN encipherment is anticipated. It is expected that early adoptions of AES will co-exist with TDEA implementations for a considerable time, and that TDEA will continue to be widely used in the industry, and approved as an algorithm for PIN encipherment. See ISO/TR 14742 for guidance on timelines for TDEA and migration to AES.

This amendment of ISO 9564-1 defines a format for extended PIN blocks together with PIN block security properties, encipherment and decipherment method, PIN block usage restrictions and translation restrictions.

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

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

AMENDMENT 1

1 Scope

This amendment provides the following:

- revisions:
  - Introduction;
  - 4.2;
  - 9.3.6;
- replacements:
  - 9.4;
- insertions:
  - 9.5. The existing 9.5 shall be renumbered 9.6.

Introduction

Delete the paragraph "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)."

4.2 Principles

Insert a new list:

- Any part of a PIN (e.g. individual digit or representations thereof) shall be subject to the same security requirements as the entire PIN as defined in this part of ISO 9564.

9.3.6 Compact PIN block usage restrictions

Replace the last part of 9.3.6 starting with the text "Table 3 illustrates...", including Table 3, with "Table 3 in 9.5 illustrates requirements c), d), and f) for PIN block translation restrictions".

9.4 Extended PIN blocks

9.4.1 General

9.4.2 specifies an extended PIN block format: format 4. Format 4 is constructed using two 128-bit fields of PIN and PAN data respectively.

When the PIN is to be enciphered using a 128-bit block cipher (e.g. AES), it shall be formatted using the PIN block format defined in this sub-clause. PIN blocks as defined in this clause shall only be enciphered using 128-bit block ciphers. Keys used for enciphering and deciphering extended PIN blocks shall be used for no other purpose.

NOTE 1 Support for 128-bit block ciphers does not imply phasing out of block ciphers currently in use, such as TDEA.

NOTE 2 The longer key length typical of 128-bit block ciphers will require additional adjustments in key distribution.

NOTE 3 As with PIN block formats 0 and 3, the plain text PAN is required in the encipherment of the PIN data as well as in the decipherment of the enciphered PIN block. In cases where the PAN is transmitted or stored in enciphered form, the plain text PAN needs to be recovered prior to usage in the processing of the format 4 PIN block.

9.4.2 Format 4 PIN block

9.4.2.1 Format 4 PIN block security properties

The format 4 PIN block satisfies the following security properties:

a) the full PAN shall be tied to the PIN block;

b) the format shall incorporate at least 64 bits of entropy;

c) the format shall incorporate at least 20 bits of redundancy that can be validated at each translation point and the point of verification;

d) modification of any bit of input shall result in an unpredictable modification of the entire enciphered PIN block.

9.4.2.2 Format 4 PIN block construction

9.4.2.2.1 General

This PIN block consists of two 128-bit fields, the plain text PIN field and the primary account number (PAN) field, including the check digit.

The format 4 PIN block shall be reversibly enciphered according to the method defined in 9.4.2.3.

9.4.2.2.2 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
C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R

where

C = Control field: is the 4-bit field value 0100 (4);

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 1010 (A);

R = Random digit: 4-bit field with a randomly selected value in the range 0000 (0) to 1111 (15).

9.4.2.2.3 Plain text primary account number field

The plain text primary account number (PAN) 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
M	A	A	A	A	A	A	A	A	A	A	A	A	A/0	A/0	A/0

65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
A/0	A/0	A/0	A/0	0	0	0	0	0	0	0	0	0	0	0	0

where

M = PAN length: 4-bit field with permissible values 0000 (zero) to 0111 (7) indicate a PAN length of 12 plus the value of the field (ranging then from 12 to 19). If the PAN is less than 12 digits, the digits are right justified and padded to the left with zeros, and M is set to 0;

A = PAN digit: 4-bit field with permissible values 0000 (zero) to 1001 (9);

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

A/0 = PAN/Pad digit: designation of these fields is determined by the PAN length field.

NOTE For format 4, the PAN is used for PIN encipherment. For devices where the PAN is captured separately from the SCD where the PIN is entered, the PAN will be transmitted to that SCD prior to the encipherment of the PIN.

9.4.2.3 Format 4 PIN block encipherment

The 128-bit plain text PIN field is enciphered with key K, and the resulting intermediate block A is added modulo-2 (XOR'd) to the 128-bit plain text PAN field. The resulting intermediate block B is enciphered with the same key K yielding the 128-bit enciphered PIN block as illustrated in Figure 1. The intermediate blocks shall not be available outside of an SCD. The random values in the plain text PIN field shall be created by means of either

a) a true random number generator, or

b) a pseudo-random number generator.

These can be achieved using a random number generator compliant with ISO/IEC 18031 and tested using NIST SP 800-22. New random values shall be used each time a PIN block is enciphered.

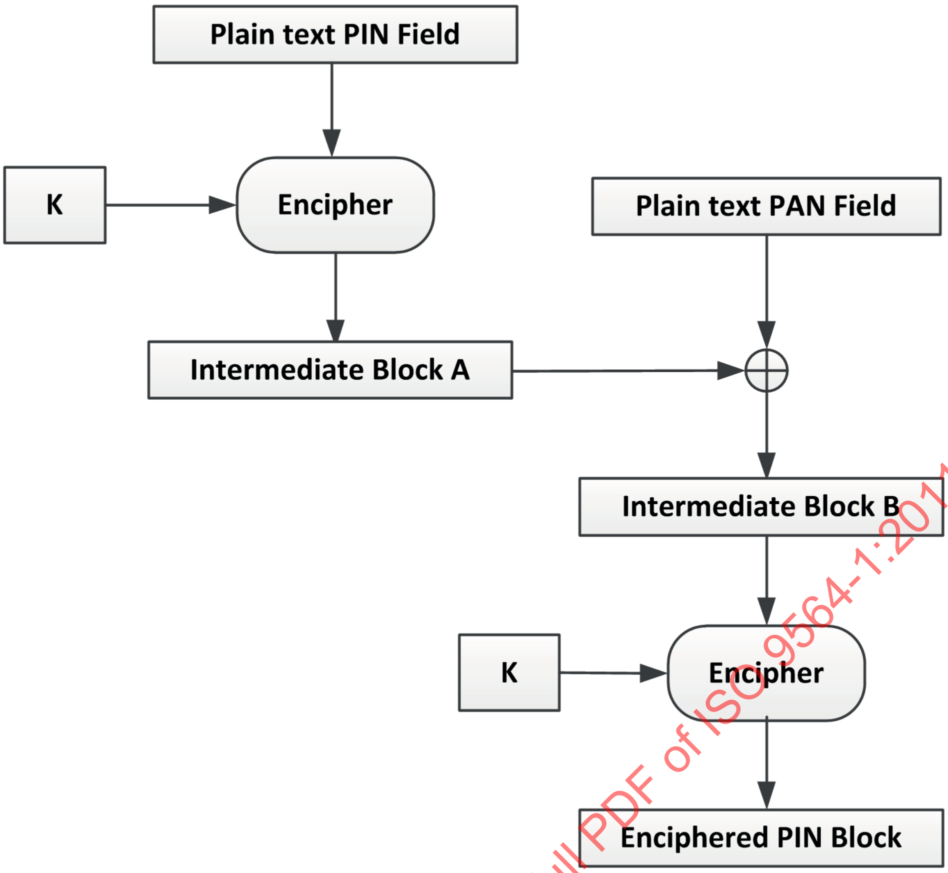

Figure 1 — Illustration of Format 4 PIN block encipherment

9.4.2.4 Format 4 PIN block decipherment

A format 4 enciphered PIN block is deciphered with key K resulting in intermediate block B, which is added modulo-2 (XOR'd) to the plain text PAN field resulting in intermediate block A. This block is deciphered with key K yielding the plain text PIN field.

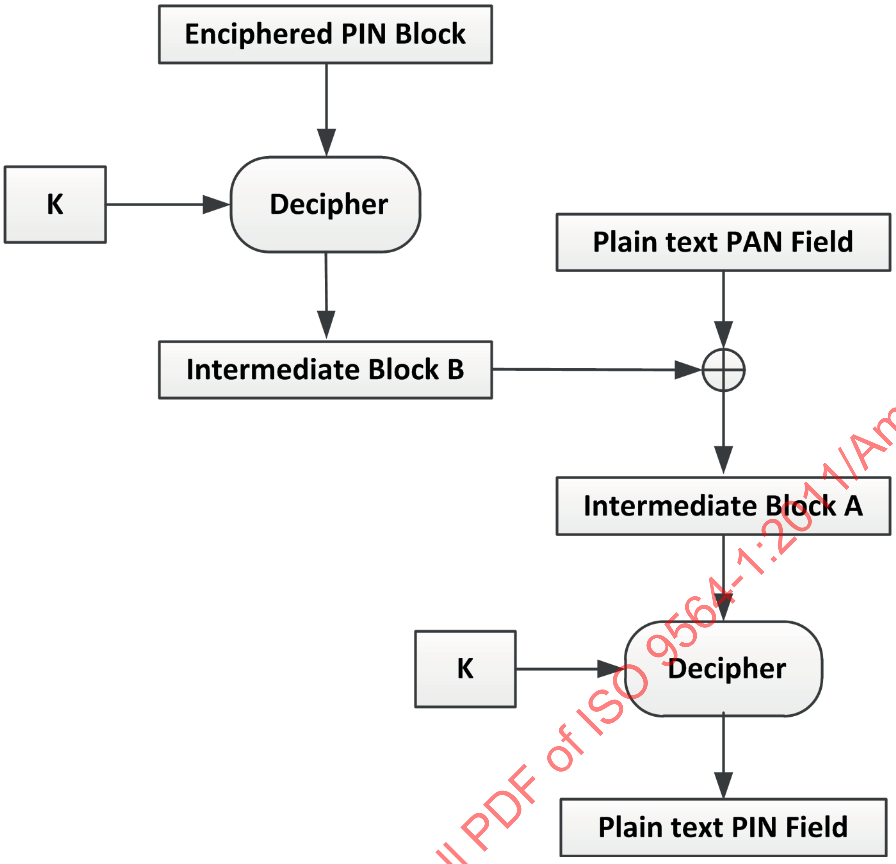

Figure 2 — Illustration of Format 4 PIN block decipherment

9.4.2.5 Format 4 PIN block usage restrictions

To ensure PIN security, the following restrictions shall apply to usage of format 4 PIN blocks.

a) Controls shall be in place to prevent the misuse of card issuance-related functions (including PIN change).

b) Format 4 PIN blocks shall not be translated into non-standard PIN block formats, or into format 1 or format 2 PIN blocks, except as specified in Table 3.

c) 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 while 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. Each time a PIN block is enciphered, new random values shall be used.

d) ISO format 4 may 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).

e) When calculating values (such as PVVs or offsets) derived from the PIN and PAN, if PAN 1 used for the derivation of the calculated value does not agree with PAN 2 used in the plain text PAN field, 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 while the host security modules are in a sensitive state and under dual control (see ISO 13491-1:2007, 6.3.6).

f) No integrity checks shall be performed on the PIN digits themselves. If integrity checks are performed on the deciphered PIN field, then they shall only be performed on the first byte of that field (control field and PIN length field) and the fill digits.