INTERNATIONAL STANDARD

ISO 9564-3

First edition
2003-11-15

Banking — Personal Identification Number management and security —

Part 3: Requirements for offline PIN handling in ATM and POS systems

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

Partie 3: Exigences relatives à la protection du PIN pour traitement du PIN hors ligne dans les systèmes ATM et POS

Reference number
ISO 9564-3:2003(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 9564-3 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

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

— *Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

— *Part 2: Approved algorithms for PIN encipherment*

— *Part 3: Requirements for offline PIN handling in ATM and POS systems*

Part 4, *Best practices for PIN handling in open networks,* is under preparation.

Introduction

Financial transaction cards with embedded integrated circuits (IC) have made it technically feasible to perform PIN verification offline using the IC card. Issuers can now choose whether to have PIN verification performed online or offline. This part of ISO 9564 provides specific requirements for addressing offline PIN handling.

Offline PIN verification does not require that a cardholder's PIN be sent to the issuer host for verification, and because of this many security requirements relating to PIN protection over networks are not applicable. However, many general PIN protection principles and techniques remain applicable even though a PIN may be verified offline. This part of ISO 9564 restricts itself to requirements relating specifically to the offline nature of PIN handling and, unless explicitly excluded, the basic principles of PIN management given in ISO 9564-1 are applicable.

ISO 10202[1] and, in particular, Part 6 of that International Standard, defines security requirements for cardholder verification using IC cards. It should be noted that ISO 10202 defines requirements for the IC card itself, rather than for the acquirer IC card acceptance systems, and so can be considered as complementary to ISO 9564.

Banking — Personal Identification Number management and security —

Part 3: Requirements for offline PIN handling in ATM and POS systems

1 Scope

This part of ISO 9564 specifies the minimum security measures required for offline Personal Identification Number (PIN) handling and a standard means of interchanging PIN data in an offline environment.

It is applicable to financial transaction, card-originated transactions requiring offline PIN verification, and to those institutions responsible for implementing techniques for the management and protection of the PIN at Automated Teller Machines (ATMs) and acquirer sponsored Point-of-Sale (POS) terminals.

This part of ISO 9564 is *not* applicable to

a) PIN management and security in the online PIN environment, which is covered in ISO 9564-1,

b) approved algorithms for PIN encipherment, which are covered in ISO 9564-2,

c) the use of PINs in an open network environment, which is to be covered in ISO 9564-4,

d) the protection of the PIN against loss or intentional misuse by the customer or authorized employees of the issuer or their agents,

e) privacy of non-PIN transaction data,

f) protection of transaction messages against alteration or substitution, e.g. an online authorization response,

g) protection against replay of the PIN or transaction,

h) specific key management techniques,

i) the decision as to whether the IC card is to receive the PIN enciphered,

j) contactless IC cards.

The basic principles of PIN management described in Clause 4 of ISO 9564-1:2002 are applicable and normative to this part of ISO 9564.

Requirements associated with multi-application IC cards are considered to be the responsibility of the issuer and are not included.

This part of ISO 9564 is framed in terms applicable to IC card technology, however, by this it is not intended to restrict its applicability to IC card technology.

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 7816 *(all parts) Identification cards — Integrated circuit(s) cards with contacts*

ISO 9564-1:2002, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

ISO 9564-2[1)], *Banking — Personal Identification Number management and security — Part 2: Approved algorithms for PIN encipherment*

ISO 11568-2, *Banking — Key Management (retail) — Part 2: Key management techniques for symmetric ciphers*

EMV2000, *Integrated Circuit Card Specification for Payment Systems, Book 2 — Security and Key Management, Version 4.0, December, 2000*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 9564-1 and the following apply.

3.1
integrated circuit
IC
microprocessor (typically) embedded in an IC card as specified in ISO 7816.

4 PIN protection during transmission between PED and IC reader

The IC reader and PIN entry device (PED) can either be two separate devices or integrated into a single device. See Table 1.

When the IC reader and PED are integrated within a device meeting the requirements of 6.3 of ISO 9564-1:2002 and the PIN is to be submitted to the IC in plain text form, then the PED need not encipher the PIN.

When the PIN is to be submitted to the IC in plain text form and is transmitted to the IC reader through an unprotected environment, then the PIN shall be enciphered in accordance with ISO 9564-1. The IC reader shall then decipher the PIN for submission in plain text to the IC.

For both integrated and non-integrated devices, when the PIN is to be submitted to the IC in enciphered form, then the PIN shall be enciphered within a device meeting the requirements of 6.3 of ISO 9564-1:2002 using an authenticated encipherment key of the IC.

If the PIN is transmitted outside of a device meeting the requirements of 6.3 of ISO 9564-1:2002, then it shall be enciphered in accordance with ISO 9564-1 or using an authenticated encipherment key of the IC.

1) To be published. (Revision of ISO 9564-2:1991)

5 Physical security

This clause gives requirements and recommendations for the physical security of PEDs and IC readers. Unless excluded below, the requirements for PEDs used for offline PIN verification are the same as those given in ISO 9564-1.

The PED should be a “physically secure device” as defined in 6.3 of ISO 9564-1:2002. If not, then, at a minimum, it shall satisfy the PED requirements of 6.3 of ISO 9564-1:2002.

In order that an attack on the PED can be detected by the acquirer, the PED should be able to authenticate itself to the acquirer such that, if attacked, it will no longer be able to authenticate itself to the acquirer.

Furthermore, if the PED is used for processing online PIN transactions (and so complies with the requirements of ISO 9564-1), then the acquirer shall verify, periodically, its integrity.

The device housing the IC reader shall satisfy the PED requirements of 6.3 of ISO 9564-1:2002.

The slot of the IC reader into which the IC card is inserted

a) should not have sufficient space to hold a PIN-disclosing “bug” when a card is in the IC reader,

b) nor should it be feasibly enlarged to provide space for a PIN-disclosing “bug”,

c) nor should it be positioned such that wires leaving the slot to an external “bug” could be hidden from users of the device.

The necessary electronic protection circuits should be provided to prevent the adding of tapping devices inside the IC reader.

Table 1 summarizes the PIN protection requirements for various terminal configurations and PIN submission methods in accordance with this clause and Clause 4.

Table 1 — PIN protection requirements

PIN submission method	PED and IC reader integrated as device in accordance with 6.3 of ISO 9564-1:2002	PED and IC reader not integrated as device in accordance with 6.3 of ISO 9564-1:2002
Enciphered PIN block submitted to IC	The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key [a] of the IC.	The PIN block shall be enciphered between the PED and the IC reader in accordance with ISO 9564-1 or enciphered using an authenticated encipherment key of the IC. The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.
Plain text PIN block submitted to IC	No encipherment is required.	The PIN block shall be enciphered from the PED to the IC reader in accordance with ISO 9564-1.
[a] See EMV2000.		