TECHNICAL REPORT

ISO/TR 9564-4

First edition
2004-03-15

Banking — Personal Identification Number (PIN) management and security —

Part 4: Guidelines for PIN handling in open networks

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

Partie 4: Directives sur la manipulation du PIN dans les dispositifs à réseau ouvert

Reference number
ISO/TR 9564-4:2004(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.

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.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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/TR 9564-4 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 (PIN) 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: Guidelines for PIN handling in open networks* [Technical Report]

Introduction

The open network environment is a high-risk environment. This is especially true for PIN-based transactions, since the management of the PIN entry device is beyond the control of either the issuer or acquirer. In many circumstances, it is the cardholder who decides on the network access device (NAD).

This part of ISO 9564 provides guidelines to assist the payment system participants in reducing the exposure of PIN compromise in open networks and the likelihood of subsequent fraud in those payment systems covered by ISO 9564-1 and ISO 9564-3. Its purpose is to define minimal PIN security practices in the open network environment. If PIN security in this environment is deficient, there is a high probability, if card data are also disclosed, that both (card data and PIN) may be fraudulently used in the ATM, POS or open network environments.

The integrity of the authentication mechanism is contingent on the confidentiality of the PIN and the cardholder data. In this environment, the lack of control makes protection of the PIN difficult; therefore, protection of the cardholder data is necessary to minimise the risk of fraud resulting from card data capture and PIN compromise in the open network environment.

Noting the fluidity of the technology and the market, it was decided that the development of an International Standard was not advised at the time of publication. This part of ISO 9564 will be reviewed on a regular basis to ensure consistency with current market requirements and technological developments.

Banking — Personal Identification Number (PIN) management and security —

Part 4: Guidelines for PIN handling in open networks

1 Scope

This part of ISO 9564 provides guidelines for personal identification number (PIN) handling in open networks, presenting finance industry best-practice security measures for PIN management and the handling of financial card originated transactions in environments where issuers and acquirers have no direct control over management, or where no relationship exists between the PIN entry device and the acquirer prior to the transaction.

It is applicable to financial card-originated transactions requiring verification of the PIN and to those organizations responsible for implementing techniques for the management of the PIN in terminals and PIN entry devices when used in open networks.

It is not applicable to

— PIN management and security in the online and offline ATM and POS PIN environments, which are covered in ISO 9564-1 and ISO 9564-3,

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

— the protection of the PIN against loss or intentional misuse by the customer or authorised employees of the issuer or their agents,

— privacy of non-PIN transaction data,

— protection of transaction messages against alteration or substitution, e.g. an online authorisation response,

— protection against replay of the PIN or transaction,

— specific key management techniques,

— access to, and storage of, card data by server-based applications such as wallets, or

— financial institution sponsored, cardholder activated, secure PIN entry devices.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
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

2.2
compromise
〈cryptography〉 breaching of secrecy and/or security

2.3
encipherment
rendering of text unintelligible by means of an encoding mechanism

2.4
integrated circuit card
ICC
ID-1 card type, as specified in ISO 7810, ISO 7811, ISO 7812 and ISO 7813, into which one or more integrated circuits have been inserted

NOTE See ISO 7816-1.

2.5
issuer
institution holding the account identified by the primary account number (PAN)

2.6
network access device
NAD
personal computer, set top box, mobile phone, PDA or other device capable of allowing access to an open network

2.7
open network
public network in which the integrity and confidentiality of transmitted data cannot be guaranteed

EXAMPLE The internet.

2.8
personal identification number
PIN
code or password possessed by the customer for verification of identity

2.9
PIN entry device
PED
PIN pad
PIN entry keypad
device into which the cardholder inputs the PIN

2.10
primary account number
PAN
assigned number that identifies the card issuer and cardholder, composed of an issuer identification number, individual account identification and accompanying check digit, as defined in ISO/IEC 7812-1

3 Open network model

3.1 Network model

Other International Standards, including ISO 9564-1 and ISO 9564-3, address PIN security for online and offline PIN-based transactions in an ATM (automatic teller machine) or POS (point-of-sale) environment.

Technological developments have now made feasible the use of PIN-based financial transactions in open networks.

In the open network environment the network access device (NAD) may initiate a transaction with any open-network-connected merchant in the world, and this merchant may use any open network-equipped acquirer. Therefore, when a PIN is used for cardholder verification in an open network transaction, the transaction acquirer has no control over the PIN-entry device into which the PIN is entered. This differs from the ATM and POS environments where the acquirer is solely responsible for the operation and security of the PIN-entry device.

3.2 Open network access devices

This part of ISO 9564 specifies the means to achieve a minimally acceptable level of security when a PIN is used for authentication in conjunction with an open network access device.

The following payment flow is assumed.

a) The cardholder contacts the merchant using a network access device that communicates via an open network.

b) The merchant communicates with its acquirer either via an open network or through normal merchant-to-acquirer communications.

c) The acquirer communicates with the issuer using the conventional authorization and settlement networks.

This part of ISO 9564 addresses the minimum security recommendation for PIN entry in these open network access devices. The information in this part of ISO 9564 provides a methodology for the protection of card data, limiting the risk of fraud within the open network access devices, since all of the devices covered are assumed to be untrusted.

Although methods of cardholder verification other than PINs are outside the scope of this part of ISO 9564, it should not be construed as implying that such other methods are less desirable than PINs.

4 Principles of PIN security in open network devices

4.1 Overview

Historically, the principles of PIN security have been based upon the confidentiality of the PIN without providing for the protection of the magnetic stripe data on the card. In this open network environment, it is difficult to ensure the confidentiality of the PIN. Consequently, in order to limit the potential risks of PIN compromise, this part of ISO 9564 focuses on the protection of the magnetic stripe data by not allowing the use of devices that provide magnetic stripe capability.

Under no circumstances should card data be stored in any device outside of the acquiring and issuing financial institutions' systems.

If the security of the system is to be maintained, it is essential that the information released by the ICC not be sufficient to permit the production of a fraudulent magnetic stripe card, for example, by ensuring that the card data authentication values in the magnetic stripe and ICC environments differ.

4.2 Card data sources

4.2.1 Integrated circuit cards

The risk of fraud is greatly reduced in the offline PIN open network environment, where no magnetic stripe capability exists, as the ICC provides significant protection for the card data. As a result, the requirement to provide robust PIN security is diminished in comparison to the requirements of ISO 9564-1 and ISO 9564-3.

4.2.2 Magnetic stripe cards

The use of magnetic stripe cards in this environment is not supported, as such use risks the security of PINs in those environments that are the subjects of ISO 9564-1 and ISO 9564-3. See Table 1 for supported and unsupported environments.

4.2.3 Manual PAN entry

When card data is manually entered, it is essential that the NAD not prompt for PIN entry.

Table 1 — Supported and unsupported environments

	NAD	
	Online PIN	**Offline PIN**
ICC	Not supported	Supported
Magnetic stripe	Not supported	Not supported
Manual PAN entry	Not supported	Not supported

5 Minimally acceptable PED

The application of the principles presented in Clause 4 results in the supported environment shown in Table 1. In order to provide the functionality for the supported environment, a device conforming to the requirements of a minimally acceptable PED (PIN entry device) as defined in the present clause is needed.

A minimally acceptable PED is a NAD that includes an ICC reader and an input device capable of allowing the cardholder to enter his/her PIN for offline verification.

It is recommended that the appropriate physical and/or cryptographic protection of the PIN be provided between the PED and the ICC. 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) not feasibly be enlarged to provide space for a PIN-disclosing “bug”, and

c) not be positioned such that wires leaving the slot to an external “bug” could be hidden from users of the device.

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

6 PIN security for offline PIN handling devices connected to open networks

6.1 General

The only environment supported by this part of ISO 9564 consists of the use of an ICC with a PED. This clause addresses offline PIN handling in an ICC environment.

6.2 Offline PIN verification at open network access devices

When offline PIN verification is performed by an ICC, the PIN is usually transmitted from the PIN entry keypad to the ICC as plaintext. Some payment applications require the submission of an enciphered PIN to the ICC using a public key of the ICC. In such situations, where the network access device is capable of performing this encipherment, the transaction will be completed.

To assist in preventing fraudulent access to the ICC, it is recommended that cardholders be instructed to remove the ICC between transactions; alternatively, the payment application should require that the card be physically reset between each transaction.

6.3 General recommendations for open network financial transactions

It is strongly recommended that cardholders be instructed to control access to their IC cards at all times when these are used in open networks. For example, cardholders should not leave their card in the NAD any longer than for the time necessary to complete the transaction.

It is strongly recommended that PEDs used in NADs be constructed such as to prevent the plaintext PIN leaving the PED except for when it is to be sent to the ICC.

Bibliography

[1] ISO/IEC 7810:2003, *Identification cards — Physical characteristics*

[2] ISO/IEC 7811 (all parts), *Identification cards — Recording technique*

[3] ISO/IEC 7812-1:2000, *Identification cards — Identification of issuers — Part 1: Numbering system*

[4] ISO/IEC 7812-2:2000, *Identification cards — Identification of issuers — Part 2: Application and registration procedures*

[5] ISO/IEC 7813:2001, *Identification cards — Financial transaction cards*

[6] ISO/IEC 7816-1:1998, *Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics*

[7] ISO 13491-1:1998, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ICS 35.240.40

Price based on 6 pages