INTERNATIONAL STANDARD

ISO 9564-1

Third edition
2011-02-15

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

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

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

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

Reference number
ISO 9564-1:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword 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 encipherment*[1)]

— *Part 3: Requirements for offline PIN handling in ATM and POS systems* [Withdrawn and incorporated into Part 1]

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

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

Introduction

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

The objective of PIN management is to protect the PIN against unauthorized disclosure, compromise and misuse throughout its life cycle and, in so doing, to minimize the risk of fraud occurring within electronic funds transfer (EFT) systems. The secrecy of the PIN needs to be assured at all times during its life cycle, which consists of its establishment, issuance, activation, storage, entry, transmission, validation, deactivation and any other use made of it.

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

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

b) delivery: PIN to the cardholder;

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

d) submission: transaction PIN to the IC card.

PIN security in part depends upon sound key management. Maintaining the secrecy of cryptographic keys is of the utmost importance because the compromise of any key allows the compromise of any PIN ever enciphered under it.

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

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

This part of ISO 9564 is designed so that issuers can uniformly make certain, to whatever degree is practical, that a PIN, while under the control of other institutions, is properly managed. Techniques are given for protecting the PIN-based customer authentication process by safeguarding the PIN against unauthorized disclosure during the PIN's life cycle.

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

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

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

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

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

1 Scope

This part of ISO 9564 specifies the basic principles and techniques which provide the minimum security measures required for effective international PIN management. These measures are applicable to those institutions responsible for implementing techniques for the management and protection of PINs during their creation, issuance, usage and deactivation.

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

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

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

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

c) privacy of non-PIN transaction data;

d) protection of transaction messages against alteration or substitution;

e) protection against replay of the PIN or transaction;

f) specific key management techniques;

g) offline PIN verification used in contactless devices;

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

3.1
acquirer
institution (or its agent) that acquires from the card acceptor the financial data relating to the transaction and initiates such data into an interchange system

3.2
algorithm
clearly specified mathematical process for computation

3.3
card acceptor
party accepting the card and presenting transaction data to an acquirer

3.4
cardholder PIN
PIN known by the cardholder

3.5
cipher text
data in their enciphered form

3.6
compromise
〈cryptography〉 breaching of confidentiality and/or integrity

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

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