INTERNATIONAL

ISO

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 2011

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.

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 9564-1 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).