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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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.