INTERNATIONAL STANDARD

ISO 9564-4

First edition
2016-03-01

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

Part 4: Requirements for PIN handling in eCommerce for Payment Transactions

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

Partie 4: Exigences pour la manipulation PIN dans le commerce électronique pour les transactions de paiement

Reference number
ISO 9564-4:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

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 algorithms for PIN encipherment*

— *Part 4: Requirements for PIN handling in eCommerce for Payment Transactions*

Introduction

The eCommerce environment is inherently high-risk. This is especially true for PIN-based transactions because if PIN security in this environment is deficient, there is a high probability, in some cases, that card and PIN data might be fraudulently captured and reused in the ATM, POS or eCommerce environments.

For conducting eCommerce transactions, cardholders use network access devices (NAD) of their choice. ISO 9564-1 prohibits PINs from being entered on NADs.

This part of ISO 9564 defines minimum security requirements and practices for acceptable devices used for the entry of the PINs in the eCommerce environment:

— devices that are compliant with ISO 9564-1 (i.e. PEDs);

— devices that are not compliant with ISO 9564-1 but are functionally secure devices for PIN entry (FSPED) for exclusive use with IC cards;

— devices that are not compliant with ISO 9564-1 but are IC cards with integrated keypad and display (ICCPED).

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

Part 4: Requirements for PIN handling in eCommerce for Payment Transactions

1 Scope

This part of ISO 9564 provides requirements for the use of personal identification numbers (PIN) in eCommerce. The PINs in scope are the same cardholder PINs used as a means of cardholder verification in card-based financial transactions; notably, automated teller machine (ATM) systems, point-of-sale (POS) terminals, automated fuel dispensers, and vending machines.

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 eCommerce.

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

— passwords, passcodes, pass phrases and other shared secrets used for customer authentication in online banking, telephone banking, digital wallets, mobile payment, etc.,

— 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, which are covered in ISO 9564-1,

— card proxies such as mobile phones or key fobs,

— 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 authorized employees of the issuer,

— privacy of non-PIN transaction data,

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

— protection against replay of the transaction,

— functionality of devices used for PIN entry which is related to issuer functions other than PIN entry,

— specific key management techniques, and

— access to, and storage of, card data other than the PIN by applications such as wallets.

2 Normative references

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

ISO 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

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
compromise
⟨cryptography⟩ breaching of confidentiality and/or integrity

3.3
contact IC reader
reader of an IC card that requires the insertion of the card into the contact IC reader to establish communication between the contact IC reader and the IC card through a physical connection

3.4
eCommerce
buying and selling of products or services over open networks

3.5
encipherment
transformation of intelligible data (plaintext) into an unintelligible form (ciphertext)

3.6
functionally secure PIN entry device
FSPED
device that communicates with a contact IC card for the purpose of using the PIN to generate an OTT offline, containing

— a contact IC reader,

— an integrated numeric keypad, and

— an alpha-numeric display

Note 1 to entry: An FSPED is not a PED in the sense of ISO 9564-1.

3.7
integrated circuit card
ICC
IC card
ID-1 card type, as specified in ISO/IEC 7816 (all parts) into which one or more integrated circuits have been inserted

3.8
integrated circuit card PIN entry device
ICCPED
ID-1 card type, as specified in ISO/IEC 7816 (all parts) into which one or more integrated circuits have been inserted, but which additionally is self-powered, has integrated keypad and display capabilities, for the purpose of using a PIN to generate an OTT offline

Note 1 to entry: Standards that describe these kinds of devices are under development (see Reference [8]).

Note 2 to entry: An ICCPED is not a PED in the sense of ISO 9564-1

