Pangandus. Isikunumbri (PIN-koodi) haldus ja turve. Osa 1: PIN-koodi kaitse põhimõtted ja meetodid

Banking - Personal Identification Number management and security - Part 1: PIN protection principles and techniques

EESTI STANDARDIKESKUS EVS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-EN 29564-1:2000 sisaldab Euroopa standardi EN 29564-1:1993 ingliskeelset teksti.	This Estonian standard EVS-EN 29564-1:2000 consists of the English text of the European standard EN 29564-1:1993.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 31.08.1993.	Date of Availability of the European standard is 31.08.1993.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.240.40

Võtmesõnad: algorithms, bank accounts, banking, coded representation, identification methods, protection of information, registration number,

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 29564-1:1993

August 1993

UDC 336.717:351.755.6:003.26

Descriptors: Banking, information interchange, bank accounts, management, registration number, personal identification number, protection of information

English version

Banking - Personal Identification Number management and security - Part 1: PIN protection principles and techniques (ISO 9564-1:1991)

Banque - Gestion et sécurité du numéro personnel d'identification - Partie 1: Principes et techniques de protection du PIN (ISO 9564-1:1991)

Bankwesen - PIN-Ausgabe und -Verwaltung und PIN-Sicherheit - Teil 1: Grundsätze und Verfahren zum Schutz der PIN (ISO 9564-1:1991)

This European Standard was approved by CEN on 1993-08-13. CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CEN member.

The European Standards exist in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Central Secretariat: rue de Stassart,36 B-1050 Brussels

Foreword

On the proposal of the CEN Central Secretariat, the Technical Board has decided to submit the International Standard:

"Banking - Personal Identification Number management and security - Part 1: PIN protection principles and techniques (ISO 9564-1:1991)"

to the formal vote.

The result of the formal vote was positive.

For the time being, this document exists only in English and in French.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 1994, and conflicting national standards shall be withdrawn at the latest by February 1994.

In accordance with the CEN/CENELEC Internal Regulations, the following countries are bound to implement this European Standard:

Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

Endorsement notice

The text of the International Standard ISO 9564-1:1991 was approved by CEN as a European Standard without any modification.

INTERNATIONAL STANDARD

ISO 9564-1

First edition
1991-12-15

Banking — Personal Identification Number management and security —

Part 1: PIN protection principles and techniques

Banque — Gestion et sécurité du numéro personnel d'identification — Partie 1: Principes et techniques de protection du PIN

Reference number
ISO 9564-1:1991(E)

Contents

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Annexes

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.

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.

International Standard ISO 9564-1 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Sub-Committee SC 6, *Financial transaction cards, related media and operations*.

ISO 9564 consists of the following parts, under the general title *Banking — Personal Identification Number management and security*:

— *Part 1: PIN protection principles and techniques*

— *Part 2: Approved algorithm(s) for PIN encipherment*

Annexes A and B form an integral part of this part of ISO 9564. Annexes C, D, E, F, G and H are for information only.

Introduction

The Personal Identification Number (PIN) is a means of verifying the identity of a customer within an electronic funds transfer (EFT) system.

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 EFT systems. The secrecy of the PIN needs to be assured at all times during its life cycle which consists of its selection, issuance, activation, storage, entry, transmission, validation, deactivation, and any other use made of it.

PIN security also 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.

Wherever possible, this part of ISO 9564 specifies requirements in absolute terms. In some instances a level of subjectivity cannot be practically avoided especially when discussing the degree of level of security desired or to be achieved.

The level of security to be achieved needs to be related to a number of factors, including the sensitivity of the data concerned and the likelihood that the data will be intercepted, the practicality of any envisaged encipherment process, and the cost of providing, and breaking, a particular means of providing security. It is, therefore, necessary for each card Acceptor, Acquirer and Issuer to agree on the extent and detail of security and PIN management procedures. Absolute security is not practically achievable; therefore, PIN management procedures should implement preventive measures to reduce the opportunity for a breach in security and aim for a "high" probability of detection of any illicit access or change to PIN material should these preventive measures fail. This applies at all stages of the generation, exchange and use of a PIN, including those processes that occur in cryptographic equipment and those related to communication of PINs.

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.

This part of ISO 9564 indicates techniques for protecting the PIN against unauthorized disclosure during its life cycle and includes the following annexes:

a) annex A gives the procedure for the approval of an encipherment algorithm;

b) annex B covers general principles of key management;

c) annex C covers techniques for PIN verification;

d) annex D deals with implementation concepts for a PIN entry device;

e) annex E identifies an example of pseudo-random PIN generation;

f) annex F indicates additional guidelines for PIN pad design;

g) annex G specifies the erasing of recording media used for storage of keying material;

h) annex H gives information for customers.

In ISO 9564-2, approved encipherment algorithms to be used in the protection of the PIN are specified. Application of the requirements of this part of ISO 9564 requires bilateral agreements to be made, including the choice of algorithms specified in ISO 9564-2.

This part of ISO 9564 is one of a series that describes requirements for security in the retail banking environment, as follows:

ISO 9564-1:1991, *Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques.*

ISO 9564-2:1991, *Banking — Personal Identification Number management and security — Part 2: Approved algorithm(s) for PIN encipherment.*

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail).*

The requirements of ISO 9564 are compatible with those in ISO 8583 for the accommodation of security related data.

Banking — Personal Identification Number management and security —

Part 1:
PIN protection principles and techniques

1 Scope

This part of ISO 9564 specifies the minimum security measures required for effective international PIN management. A standard means of interchanging PIN data is provided. This part of ISO 9564 also specifies the rules related to the approval of PIN encipherment algorithms. This part of ISO 9564 is applicable to institutions responsible for implementing techniques for the management and protection of the PIN for bank card originated transactions. The provisions of this part of ISO 9564 are not intended to cover

- 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 authorization response to a PIN verification;
- protection against replay of the PIN or transaction;
- specific key management techniques;
- PIN management and security for transactions conducted using Integrated Circuit Cards (ICC);
- the use of asymmetric encipherment algorithms for PIN management.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 9564. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 9564 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7812:1987, *Identification cards — Numbering system and registration procedure for issuer identifiers.*

ISO 8583:1987, *Bank card originated messages — Interchange message specifications — Content for financial transactions.*

ISO 8908:—[1], *Banking and related financial services — Vocabulary and data elements.*

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail).*

American National Standard X3.92:1981, *Data Encryption Algorithm (DEA).*

3 Definitions

For the purposes of this part of ISO 9564, the following definitions apply.

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

3.2 algorithm: A clearly specified mathematical process for computation.

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

3.4 cipher text: Data in its enciphered form.

3.5 compromise: In cryptography, the breaching of secrecy and/or security.

3.6 cryptographic key: A mathematical value which is used in an algorithm to transform plain text into cipher text or vice versa.

3.7 customer: The individual associated with the primary account number (PAN) specified in the transaction.

3.8 decipherment: The reversal of a previous reversible encipherment, rendering cipher text intelligible.

3.9 dual control: A process of utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single entity is able to access or utilize the materials, e.g. cryptographic key.

3.10 encipherment: The rendering of text unintelligible by means of an encoding mechanism.

3.11 irreversible encipherment: Transformation of plain text to cipher text in such a way that the original plain text cannot be recovered by other than exhaustive procedures even if the cryptographic key is known.

3.12 irreversible transformation of a key: Generation of a new key from the previous key such that there is no feasible technique for determining the previous key given a knowledge of the new key and of all details of the transformation.

3.13 issuer: The institution holding the account identified by the primary account number (PAN).

3.14 key component: One of at least two parameters having the format of a cryptographic key that is added modulo-2 with one or more like parameters to form a cryptographic key.

3.15 modulo-2 addition: Binary addition with no carry (also called Exclusive OR′ing).

3.16 node: Any message processing entity through which a transaction passes.

3.17 notarization: A method of modifying a key enciphering key in order to authenticate the identities of the originator and the ultimate recipient.

3.18 Personal Identification Number (PIN): The code or password the customer possesses for verification of identity.

3.19 plain text: Data in its original unenciphered form.

[1] To be published.