

Banking — Personal Identification Number management and security —

Part 1: PIN protection principles and techniques

The European Standard EN 29564-1:1993 has the status of a
British Standard

UDC 336.717:351.755.6:003.26

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Information Systems Technology Standards Policy Committee (IST/-) to Technical Committee IST/12, upon which the following bodies were represented:

- American Banks and Securities Association of London
- Association for Payment Clearing Services
- Building Societies Association
- British Telecommunications plc
- IBM (UK) Ltd.
- The London Stock Exchange

The following bodies were also represented in the drafting of the standard, through subcommittees and panels:

- British Bankers' Association
- The EDI Association
- Institutional Fund Managers' Association
- The London Stock Exchange
- Stock Exchange Management Association
- Securities and Investments Board

This British Standard, having been prepared under the direction of the Information Systems Technology Standards Policy Committee, was published under the authority of the Standards Board and comes into effect on 28 February 1992

© BSI 10-1999

The following BSI references relate to the work on this standard:
Committee reference IST/12
Draft for comment 89/60242 DC

ISBN 0 580 20692 0

Amendments issued since publication

Amd. No.	Date	Comments
7990	February 1994	Indicated by a sideline in the margin

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	2
Foreword	iii
Text of ISO 9564-1	1

National foreword

This British Standard reproduces verbatim ISO 9564-1:1991 and implements it as the UK national standard.

In 1993 the European Committee for Standardization (CEN) accepted ISO 9564-1:1991 as European Standard EN 29564-1:1993. As a consequence of implementing the European Standard, this British Standard is renumbered as BS EN 29564-1 and any reference to BS ISO 9564-1 should be read as a reference to BS EN 29564-1.

This British Standard is published under the direction of the Information Systems Technology Standards Policy Committee whose Technical Committee IST/12 has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

NOTE International and European Standards, as well as overseas standards, are available from BSI Sales Department, BSI, Linford Wood, Milton Keynes, MK14 6LE.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the EN title page, page 2, the ISO title page, pages ii to iv, pages 1 to 22 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

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.

This European Standard exists 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

© 1993 Copyright reserved to CEN members

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.

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)

AVA **Documents**
Document Sharing Hub

Contents

	Page
Foreword	iii
Introduction	1
1 Scope	2
2 Normative references	2
3 Definitions	2
4 Basic principles of PIN management	4
5 PIN pads	5
5.1 Character set	5
5.2 Character representation	5
5.3 PIN entry	5
5.4 Packaging considerations	5
6 PIN security issues	6
6.1 PIN control procedures	6
6.2 PIN encipherment	6
6.3 Physical security	7
7 Techniques for management/protection of account-related PIN functions	7
7.1 PIN length	7
7.2 PIN selection	8
7.3 PIN delivery and issuance	8
7.4 PIN change	9
7.5 Disposal of waste material and returned PIN mailers	9
7.6 PIN activation	10
7.7 PIN storage	10
7.8 PIN deactivation	10
8 Techniques for management/protection of transaction-related PIN functions	10
8.1 PIN entry	10
8.2 Protection of PIN during transmission	10
8.3 Standard PIN block formats	10
8.4 Other PIN block formats	12
8.5 PIN verification	12
8.6 Journaling of transactions containing PIN data	12
9 Approval procedure for encipherment algorithms	12
Annex A (normative) Procedure for approval of an encipherment algorithm	13
Annex B (normative) General principles of key management	14
Annex C (informative) PIN verification techniques	15
Annex D (informative) PIN entry device	16
Annex E (informative) Example of pseudo-random PIN generation	18
Annex F (informative) Additional guidelines for PIN pad design	18
Annex G (informative) Guidance on clearing and destruction procedures for sensitive data	20
Annex H (informative) Information for customers	22
Table 1 — Character representation	5
Table 2 — PIN pad packaging considerations	6
Table F.1 — ANSI alpha-to-numeric mapping	19
Table F.2 — CCITT alpha-to-numeric mapping	20

Descriptors: Banking, bank accounts, identification methods, registration number, protection of information, coded representation, algorithms.

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*;

Annex A and Annex B form an integral part of this part of ISO 9564. Annex C, Annex D, Annex E, Annex F, Annex G and Annex 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 safe-guarding 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.