

Implementation of EN ISO 11568-2:1996

# Banking — Key management (retail) —

Part 2: Key management techniques for  
symmetric ciphers

The European Standard EN ISO 11568-2:1996 has the status of a  
British Standard

ICS 35.240.40

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

# Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee IST/12, Banking, securities and other financial services, upon which the following bodies were represented:

- Association for Payment Clearing Services (APACS)
- APACS (Bank of England)
- APACS (Barclays Bank)
- APACS (Midland Bank)
- APACS (National Westminster Bank)
- APACS (Trustee Savings Bank)

The following bodies were also represented in the drafting of the standard, through BSI Technical Subcommittee IST/12/4:

- Association for Payment Clearing Services (APACS)
- Bank of England
- Brinson and Partners
- British Bankers Association (Registrar & Receiving Agent functions)
- Electronic Trade Confirmation Industry User Group and Institutional Fund Managers Association
- Extel Financial Services
- HSBC Investment Bank plc
- International Securities Markets Association
- James Capel & Co.
- London Stock Exchange
- London Clearing House
- Securities Industry Management Association
- Securities Industry Software Association

This British Standard, having been prepared under the direction of the Information Systems Technology Assembly, was published under the authority of the Standards Board and comes into effect on 15 November 1996

© BSI 07-1999

The following BSI references relate to the work on this standard:  
Committee reference IST/12  
Draft for comment 92/66523 DC

ISBN 0 580 26437 3

## Amendments issued since publication

| Amd. No. | Date | Comments |
|----------|------|----------|
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |

# Contents

|                        | Page               |
|------------------------|--------------------|
| Committees responsible | Inside front cover |
| National foreword      | ii                 |
| Foreword               | 2                  |
| Foreword               | iii                |
| Text of ISO 11568-2    | 1                  |

## National foreword

This British Standard has been prepared by Technical Committee IST/12 and is the English language version of EN ISO 11568-2:1996 *Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers* published by the European Committee for Standardization (CEN). The European Standard was derived by CEN from ISO 11568-2:1994 published by the International Organization for Standardization (ISO).

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

- aid enquirers to understand the text;
- present to the responsible European 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 Customer Services, BSI, 389 Chiswick High Road, London W4 4AL.

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 ISO title page, page 2, the ISO title page, pages ii to iv, pages 1 to 14 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.

English version

## Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers

(ISO 11568-2:1994)

Banque — Gestion de clés (services aux particuliers) —  
Partie 2: Techniques de gestion de clés pour les algorithmes cryptographiques symétriques  
(ISO 11568-2:1994)

Bankwesen — Schlüsselerwaltung (Einzelhandel) —  
Teil 2: Schlüsselerwaltungstechniken für symmetrische Verschlüsselungen  
(ISO 11568-2:1994)

This European Standard was approved by CEN on 1996-05-29. 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

## Foreword

The text of the International Standard from Technical Committee ISO/TC 68, Banking and related financial services, of the International Organization for Standardization (ISO) has been taken over as an European Standard by Technical Committee CEN/TC 224, Machine-readable cards, related device interfaces and operations, the secretariat of which is held by AFNOR.

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 December 1996, and conflicting national standards shall be withdrawn at the latest by December 1996.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of 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 the United Kingdom.

# INTERNATIONAL STANDARD

# ISO 11568-2

First edition  
1994-12-01

---

---

## **Banking — Key management (retail) —**

### **Part 2:**

Key management techniques for symmetric  
ciphers

*Banque — Gestion de clés (services aux particuliers) —*

*Partie 2: Techniques de gestion de clés pour les algorithmes  
cryptographiques symétriques*



Reference number  
ISO 11568-2:1994(E)

**AVA** Documents  
Document Sharing Hub

## Contents

|                                                                      | Page |
|----------------------------------------------------------------------|------|
| Foreword                                                             | iii  |
| Introduction                                                         | 1    |
| 1 Scope                                                              | 1    |
| 2 Normative references                                               | 1    |
| 3 Definitions                                                        | 1    |
| 4 General environment for key management techniques                  | 2    |
| 4.1 Functionality of a secure cryptographic device                   | 2    |
| 4.2 Double length keys                                               | 3    |
| 4.3 Key generation                                                   | 4    |
| 4.4 Key calculation                                                  | 4    |
| 4.5 Key hierarchies                                                  | 4    |
| 5 Techniques for the provision of key management services            | 5    |
| 5.1 Key encipherment                                                 | 5    |
| 5.2 Key variants                                                     | 5    |
| 5.3 Key derivation                                                   | 6    |
| 5.4 Key transformation                                               | 6    |
| 5.5 Key offsetting                                                   | 7    |
| 5.6 Key notarization                                                 | 7    |
| 5.7 Key tagging                                                      | 7    |
| 5.8 Key verification                                                 | 8    |
| 5.9 Key identification                                               | 8    |
| 5.10 Controls and audit                                              | 8    |
| 6 Key management services cross reference                            | 9    |
| Annex A (normative) Notation used in this part of ISO 11568          | 10   |
| A.1 Operators                                                        | 10   |
| A.2 Suffix letters for keys                                          | 10   |
| A.3 Specific keys and key pairs                                      | 10   |
| Annex B (normative) Approved algorithms for symmetric key management | 10   |
| Annex C (normative) Abbreviations                                    | 11   |
| Annex D (informative) Symmetric cipher examples                      | 12   |
| Annex E (informative) Key variants and control vectors               | 13   |
| E.1 Key variants                                                     | 13   |
| E.2 Control vectors                                                  | 14   |
| Annex F (informative) Bibliography                                   | 14   |
| Figure 1 — Use of double length keys                                 | 3    |
| Figure 2 — Variant key calculation                                   | 5    |
| Figure 3 — Generation of a derived key                               | 6    |
| Figure 4 — Generation of future keys                                 | 6    |
| Figure 5 — Calculation of a KEK offset (KEKo)                        | 7    |
| Figure 6 — Tagged key generation                                     | 7    |
| Figure 7 — Tagged key use                                            | 7    |
| Figure 8 — Example of KVC function                                   | 8    |
| Figure D.1 — Example of a symmetric cipher key management system     | 12   |
| Figure E.1 — Example of Control Vectors for “function x”             | 14   |
| Table 1                                                              | 9    |
| Table D.1 — Examples of key usage at node B                          | 13   |