

Implementation of
ISO 10126-1:1991

Banking — Procedures for message encipherment (wholesale) —

Part 1: General principles

UDC 336.719.2:355.405.2:681.3.04

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

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 31 January 1992

© BSI 10-1999

The following BSI references relate to the work on this standard:
Committee reference IST/12
Draft for comment 89/63555 DC

ISBN 0 580 20452 9

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	iii
Text of ISO 10126-1	1

National foreword

This British Standard reproduces verbatim ISO 10126-1:1991 and implements it as the UK national standard.

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 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.

INTERNATIONAL STANDARD

ISO
10126-1

First edition
1991-11-01

Banking — Procedures for message encipherment (wholesale) —

Part 1: General principles

*Banque — Procédures de chiffrement de messages (service aux
entreprises) —*

Partie 1: Principes généraux



Reference number
ISO 10126-1:1991(E)

AVA **Documents**
Document Sharing Hub

Contents

	Page
Foreword	iii
Introduction	1
1 Scope	1
2 Normative references	1
3 Definitions	1
4 Application	2
5 Encipherment and decipherment of entire messages and encipherment elements	3
6 Transparent transmission of enciphered data	5
7 Order of processing	8
8 Approval procedure for encipherment algorithms	8
Annex A (normative) Procedure for review of alternative encipherment algorithms	9
Annex B (informative) Examples of filtering	10
Annex C (informative) Filtering — Expansion factors for selected filters	12
Annex D (informative) Examples illustrating the encipherment and decipherment of encipherment elements	13
Figure 1 — Filter padding field format	7
Figure 2 — Message flow	8
Table 1 — ISO 646 filter	5
Table 2 — ISO 646/ baudot filter	6
Table 3 — ISO 646/ baudot filter	7
Table 4 — Filter padding	7
Table C.1 — Expansion factors	12

Descriptors: Banking, messages, protection of information, coded representation.

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 10126-1 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Sub-Committee SC 2, *Operations and procedures*.

ISO 10126 consists of the following parts, under the general title *Banking — Procedures for message encipherment (wholesale)*:

- *Part 1: General principles*;
- *Part 2: DEA algorithm*.

ISO 10126 originates from work done in ANSI, and is a development of (while remaining compatible with) ANSI X9.23 (1988), *Financial Institution: Encryption of Wholesale Financial Messages*.

The four annexes to this parts of ISO 10126 are intended to simplify its implementation.

- a) Annex A provides the procedure for review of alternative encipherment algorithms.
- b) Annex B provides examples of the various filtering techniques described in this part of ISO 10126.
- c) Annex C provides a comparison of the effects of the filters described in this part of ISO 10126 and, by use of the expansion factor, shows the relationship between the number of bits transmitted and those originated.
- d) Annex D provides examples of the three methods for encipherment and decipherment of encipherment elements within a message which are described in this part of ISO 10126.

Annex A forms an integral part of this part of ISO 10126. Annex B, Annex C and Annex D are for information only.

