

Implementation of
ISO/IEC 9796:1991

Information technology — Security techniques — Digital signature scheme giving message recovery

UDC 681.3:621.39

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/33, upon which the following bodies were represented:

- Association for Payment Clearing Services
- Bull Hn Information Systems Ltd.
- CCTA (the Government Centre for Information Systems)
- Department of Trade and Industry (It Standards Unit)(It d6a)
- GCHQ (CESG)
- IBM United Kingdom Ltd.
- International Computers Limited
- Rank Xerox Ltd.

The following body was also represented in the drafting of the standard, through subcommittees and panels:

British Telecommunications plc

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 15 March 1994

© BSI 08-1999

The following BSI references relate to the work on this standard:
Committee reference IST/33
Draft for comment 90/62644 DC

ISBN 0 580 22860 6

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	iii
Text of ISO/IEC 9796	1

National foreword

This British Standard reproduces verbatim ISO/IEC 9796:1991 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/33 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 Customer Services, Publications, 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/IEC 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/IEC
9796

First edition
1991-09-15

Information technology — Security techniques — Digital signature scheme giving message recovery

*Technologies de l'information — Techniques de sécurité — Schéma de
signature numérique rétablissant le message*



Reference number
ISO/IEC 9796:1991(E)

AVA Documents
Document Sharing Hub

Contents

	Page
Foreword	iii
Introduction	1
1 Scope	1
2 Definitions	1
3 Symbols and abbreviations	1
4 General overview	2
5 Signature process	2
6 Verification process	3
Annex A (informative) Example of a public-key system for digital signature	5
Annex B (informative) Illustrative examples related to Annex A	6
Annex C (informative) Some precautions taken against various potential attacks related to Annex A	14
Annex D (informative) Bibliography	14
Figure 1 — Signature process	2
Figure 2 — Verification process	3
Table 1 — Permutation Π and shadow S	4

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 9796 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Annex A, Annex B, Annex C and Annex D are for information only.

