

Implementation of  
ISO/IEC 9797:1994

**Information  
technology —  
Security techniques —  
Data integrity  
mechanism using a  
cryptographic check  
function employing a  
block cipher algorithm**

UDC 681.3.04:003.26

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
- CCTA (the Government Centre for Information Systems)
- Department of Trade and Industry [It Standards Unit (It6a)]
- GCHQ
- GCHQ (CESG)
- IBM United Kingdom Ltd.
- International Computers Limited
- Ministry of Defence
- Rank Xerox Ltd.

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 November 1994

© BSI 04-2000

First published October 1990  
Second edition November 1994

The following BSI references relate to the work on this standard:  
Committee reference IST/33  
Draft for comment 93/640639 DC

ISBN 0 580 23505 X

## Amendments issued since publication

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

# Contents

|                        | Page               |
|------------------------|--------------------|
| Committees responsible | Inside front cover |
| National foreword      | ii                 |
| Foreword               | iii                |
| Text of ISO/IEC 9797   | 1                  |

## National foreword

This British Standard reproduces verbatim ISO/IEC 9797:1994 and implements it as the UK national standard.

This revision supersedes BS ISO/IEC 9797:1990, which is now withdrawn.

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, Sales Department, 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 ISO/IEC title page, pages ii to iv, pages 1 to 8 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.

---

---

**Information technology — Security  
techniques — Data integrity mechanism  
using a cryptographic check function  
employing a block cipher algorithm**

*Technologies de l'information — Techniques de sécurité — Mécanisme  
d'intégrité des données utilisant une fonction de contrôle cryptographique  
employant un algorithme de chiffrement par bloc*



Reference number  
ISO/IEC 9797:1994(E)

Contents

|                                        | Page |
|----------------------------------------|------|
| Foreword                               | iii  |
| Introduction                           | 1    |
| 1 Scope                                | 1    |
| 2 Normative references                 | 1    |
| 3 Definitions and notation             | 1    |
| 4 Requirements                         | 1    |
| 5 MAC calculation                      | 1    |
| Annex A (normative) Optional Processes | 4    |
| Annex B (informative) Examples         | 6    |
| Annex C (informative) Bibliography     | 8    |
| Figure 1 — The MAC calculation         | 3    |
| Figure A.1 — Optional process 1        | 4    |
| Figure A.2 — Optional process 2        | 5    |