

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)

Contents

	Page
Foreword	iii
Introduction	iv
1 Scope	1
2 Definitions	1
3 Symbols and abbreviations	1
4 General overview	1
5 Signature process	2
6 Verification process	3

Annexes

A Example of a public-key system for digital signature	4
B Illustrative examples related to annex A	6
C Some precautions taken against various potential attacks related to annex A	11
D Bibliography	12