

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

National foreword

This British Standard reproduces verbatim ISO/IEC 14888-1:1998 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

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 11 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.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 April 1999

© BSI 02-2000

ISBN 0 580 32217 3

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
National foreword	Inside front cover
Foreword	iii
Text of ISO/IEC 14888-1	1

INTERNATIONAL STANDARD

ISO/IEC 14888-1

First edition
1998-12-15

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

*Technologies de l'information — Techniques de sécurité — Signatures
digitales avec appendice —*

Partie 1: Généralités



Contents

	Page
Foreword	iii
Introduction	1
1 Scope	1
2 Normative references	1
3 General	1
4 Terms and definitions	1
5 Symbols, conventions, and legend for figures	3
5.1 Symbols	3
5.2 Coding convention	3
5.3 Legend for figures	3
6 General model	3
7 Options for binding signature mechanism and hash-function	4
8 Key generation process	4
9 Signature process	5
9.1 Producing pre-signature	6
9.2 Preparing message	6
9.3 Computing witness	7
9.4 Computing signature	7
10 Verification process	7
10.1 Preparing message	7
10.2 Retrieving witness	7
10.3 Computing verification function	9
10.4 Verifying witness	9
11 Randomized mechanisms with two-part signatures	9
11.1 Computing signature	9
11.1.1 Computing the first part of the signature	10
11.1.2 Computing assignment	10
11.1.3 Computing the second part of the signature	10
11.2 Computing verification function	10
11.2.1 Retrieving assignment	10
11.2.2 Recomputing pre-signature	10
11.2.3 Retrieving assignment	11
11.2.4 Recomputing pre-signature	11
11.2.5 Recomputing witness	11
Figure 1 — Signed message	4
Figure 2 — Signature process with a deterministic witness	5
Figure 3 — Signature process with a randomized witness	6
Figure 4 — Verification process with a deterministic witness	8
Figure 5 — Verification process with a randomized witness	8
Figure 6 — Computing the signature in a randomized mechanism with a deterministic witness	9
Figure 7 — Computing the signature with a randomized witness as part of the signature	9
Figure 8 — Computing verification function of a randomized mechanism with a deterministic witness	10
Figure 9 — Computing verification function with a randomized witness as part of the signature	11