

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

ICS 35.040

National foreword

This British Standard is the UK implementation of ISO/IEC 14888-1:2008. It supersedes BS ISO/IEC 14888-1:1998 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT — Security techniques.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 May 2008

© BSI 2008

ISBN 978 0 580 54258 9

Amendments/corrigenda issued since publication

Date	Comments

INTERNATIONAL STANDARD

ISO/IEC 14888-1

Second edition
2008-04-15

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

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

Partie 1: Généralités

Reference number
ISO/IEC 14888-1:2008(E)



AVA Documents
Document Sharing Hub

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols, conventions, and legend for figures.....	3
4.1 Symbols	3
4.2 Coding convention	4
4.3 Legend for figures	4
5 General.....	4
6 General model	5
7 Options for binding signature mechanism and hash-function.....	6
8 Key generation	6
9 Signature process.....	7
9.1 General.....	7
9.2 Computing the signature	7
9.3 Constructing the appendix	7
9.4 Constructing the signed message.....	7
10 Verification process	8
Annex A (informative) On hash-function identifiers	10
Bibliography	11

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 14888-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 14888-1:1998), which has been technically revised.

ISO/IEC 14888 consists of the following parts, under the general title *Information technology — Security techniques — Digital signatures with appendix*:

- *Part 1: General*
- *Part 2: Integer factorization based mechanisms*
- *Part 3: Discrete logarithm based mechanisms*