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)

© ISO/IEC 2008

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

 © ISO/IEC 2008 – All rights reserved

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

© ISO/IEC 2008 – All rights reserved

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*

 © ISO/IEC 2008 – All rights reserved

Introduction

Digital signature mechanisms are asymmetric cryptographic techniques which can be used to provide entity authentication, data origin authentication, data integrity and non-repudiation services. There are two types of digital signature mechanisms:

— When the verification process needs the message as part of the input, the mechanism is called a "signature mechanism with appendix". A hash-function is used in the calculation of the appendix.

— When the verification process reveals all or part of the message, the mechanism is called a "signature mechanism giving message recovery". A hash-function is also used in the generation and verification of these signatures.

Signature mechanisms with appendix are specified in ISO/IEC 14888. Signature mechanisms giving message recovery are specified in ISO/IEC 9796. Hash-functions are specified in ISO/IEC 10118.

© ISO/IEC 2008 – All rights reserved

Information technology — Security techniques — Digital signatures with appendix —

Part 1: General

1 Scope

ISO/IEC 14888 specifies several digital signature mechanisms with appendix for messages of arbitrary length.

This part of ISO/IEC 14888 contains general principles and requirements for digital signatures with appendix. It also contains definitions and symbols which are used in all parts of ISO/IEC 14888.

Various means are available to obtain a reliable copy of the public verification key, e.g., a public key certificate. Techniques for managing keys and certificates are outside the scope of ISO/IEC 14888. For further information, see ISO/IEC 9594-8 [4], ISO/IEC 11770-3 [3] and ISO/IEC 15945 [5].

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

None.

© ISO/IEC 2008 – All rights reserved