INTERNATIONAL STANDARD

ISO/IEC 14888-2

Second edition
2008-04-15

Information technology — Security techniques — Digital signatures with appendix

Part 2: Integer factorization based mechanisms

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

Partie 2: Mécanismes basés sur une factorisation entière

Reference number
ISO/IEC 14888-2:2008(E)

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

Contents

Page

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.

ISO/IEC 14888-2 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 14888-2:1999), 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*

Introduction

Digital signatures can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and data integrity.

NOTE There are two series of International Standards specifying digital signatures. In both series, Part 2 specifies integer factorization based mechanisms and Part 3 specifies discrete logarithm based mechanisms.

- ISO/IEC 9796 [2], specifies signatures giving message recovery. As all or part of the message is recovered from the signature, the recoverable part of the message is not empty. The signed message consists of either the signature only (when the non-recoverable part of the message is empty), or both the signature and the non-recoverable part.
- ISO/IEC 14888 specifies signatures with appendix. As no part of the message is recovered from the signature, the recoverable part of the message is empty. The signed message consists of the signature and the whole message.

Most digital signature schemes involve three basic operations.

- An operation that produces key pairs. Each pair consists of a private signature key and a public verification key.
- An operation that makes use of a private signature key to produce signatures.
  - When, for a given message and private signature key, the probability of obtaining the same signature twice is negligible, the operation is probabilistic.
  - When, for a given message and private signature key, all the signatures are identical, the operation is deterministic.
- A deterministic operation that makes use of a public verification key to verify signed messages.

For each scheme, given the public verification key (but not the private signature key) and any set of signed messages (each message having been chosen by the attacker), the attacker should have a negligible probability of producing:

- a new signature for a previously signed message;
- a signature for a new message;
- the private signature key.

The title of ISO/IEC 14888-2 has changed, from *Identity-based mechanisms* (first edition) to *Integer factorization based mechanisms* (second edition).

a) The second edition includes the identity-based scheme specified in ISO/IEC 14888-2:1999, namely the GQ1 scheme. This scheme has been revised due to the withdrawal of ISO/IEC 9796:1991 in 1999.

b) Among the certificate-based schemes specified in ISO/IEC 14888-3:1998, it includes all the schemes based on the difficulty of factoring the modulus in use, namely, the RSA, RW and ESIGN schemes. These schemes have been revised due to the withdrawal of ISO/IEC 9796:1991 in 1999.

c) It takes into account ISO/IEC 14888-3:1998/Cor.1:2001, technical corrigendum to the ESIGN scheme.

d) It includes a format mechanism, namely the PSS mechanism, already specified in ISO/IEC 9796-2:2002, and details of how to use it in each of the RSA, RW, GQ1 and ESIGN schemes.

NOTE Similar format mechanisms have proofs of security [2], even without a salt.

e) It includes new certificate-based schemes that use no format mechanism, namely, the GQ2, GPS1 and GPS2 schemes.

f) For each scheme and its options, as needed, it provides an object identifier.

ISO and IEC draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from the companies listed below:

Patent holder	Patent number(s)	Subject
NTT 20-2 Nishi-shinjuku 3-Chome Shinjuku-ku Tokyo 163-1419, Japan	US 4 625 076	ESIGN (see Clause 11)
France Telecom R&D [a] Service PIV 38-40 Rue du Général Leclerc F 92794 Issy les Moulineaux Cedex 9, France	US 5 140 634, EP 0 311 470 EP 0 666 664	GQ1 (see Clause 7) GPS1 (see Clause 9)
Philips International B.V. Corporate Patents and Trademarks P.O. Box 220 5600 AE Eindhoven, The Netherlands	US 5 140 634, EP 0 311 470	GQ1 (see Clause 7)
University of California Senior Licensing Officer Office of Technology Transfer 1111 Franklin Street, 5th floor Oakland, California 94607-5200, USA	US 6 266 771	PSS (see 6.4 when using salt and 11.4)

[a] France Telecom claims that patent applications are pending in relation to GQ2 (see Clause 8) and GPS2 (see Clause 10). The patent numbers will be provided when available. ISO/IEC will then request the appropriate statements.

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

Information technology — Security techniques — Digital signatures with appendix

Part 2:
Integer factorization based mechanisms

1 Scope

This part of ISO/IEC 14888 specifies digital signatures with appendix whose security is based on the difficulty of factoring the modulus in use. For each signature scheme, it specifies:

a) the relationships and constraints between all the data elements required for signing and verifying;

b) a signature mechanism, i.e., how to produce a signature of a message with the data elements required for signing;

c) a verification mechanism, i.e., how to verify a signature of a message with the data elements required for verifying.

The production of key pairs requires random bits and prime numbers. The production of signatures often requires random bits. Techniques for producing random bits and prime numbers are outside the scope of this part of ISO/IEC 14888. For further information, see ISO/IEC 18031 [33] and ISO/IEC 18032 [34].

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 this part of ISO/IEC 14888. For further information, see ISO/IEC 9594-8 [27], ISO/IEC 11770 [31] and ISO/IEC 15945 [32].

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.

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

ISO/IEC 14888-1, *Information technology — Security techniques — Digital signatures with appendix — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 14888-1 and the following apply.

3.1
modulus
integer whose factorization shall be kept secret and whose factors shall be infeasible to compute