INTERNATIONAL STANDARD

ISO/IEC 9796-2

Second edition
2002-10-01

Information technology — Security techniques — Digital signature schemes giving message recovery —

Part 2: Integer factorization based mechanisms

Technologies de l'information — Techniques de sécurité — Schémas de signature numérique rétablissant le message —

Partie 2: Mécanismes basés sur une factorisation entière

Reference number
ISO/IEC 9796-2:2002(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.ch
Web www.iso.ch

Printed 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 3.

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 9796-2 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 9796-2:1997), which has been technically revised. Implementations which comply with ISO/IEC 9796-2 (1st edition), and which use a hash-code of at least 160 bits in length, will be compliant with ISO/IEC 9796-2 (2nd edition). Note, however, that implementations complying with ISO/IEC 9796-2 (1st edition) that use a hash-code of less than 160 bits in length will not be compliant with ISO/IEC 9796-2 (2nd edition).

ISO/IEC 9796 consists of the following parts, under the general title *Information technology — Security techniques — Digital signature schemes giving message recovery*:

— *Part 1: Mechanisms using redundancy*

— *Part 2: Integer factorization based mechanisms*

— *Part 3: Discrete logarithm based mechanisms*

Further parts may follow.

Annexes A and B form a normative part of this part of ISO/IEC 9796. Annexes C and D are for information only.

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and integrity of data. A digital signature mechanism satisfies the following requirements.

- Given the verification key but not the signature key it shall be computationally infeasible to produce a valid signature for any message.
- Given the signatures produced by a signer, it shall be computationally infeasible to produce a valid signature on a new message or to recover the signature key.
- It shall be computationally infeasible, even for the signer, to find two different messages with the same signature.

NOTE Computational feasibility depends on the specific security requirements and environment.

Most digital signature mechanisms are based on asymmetric cryptographic techniques and involve three basic operations.

- A process for generating pairs of keys, where each pair consists of a private signature key and the corresponding public verification key.
- A process that uses the signature key, called the signature process.
- A process that uses the verification key, called the verification process.

There are two types of digital signature mechanisms.

- When, for a given signature key, two signatures produced for the same message are identical, the mechanism is said to be non-randomized (or deterministic); see ISO/IEC 14888-1.
- When, for a given message and signature key, each application of the signature process produces a different signature, the mechanism is said to be randomized.

The first and third of the three mechanisms specified in this part of ISO/IEC 9796 are deterministic (non-randomized), whereas the second of the three mechanisms specified is randomized.

Digital signature mechanisms can also be divided into the following two categories:

- When the whole message has to be stored and/or transmitted along with the signature, the mechanism is named a “signature mechanism with appendix” (see ISO/IEC 14888).
- When the whole message, or part of it, can be recovered from the signature, the mechanism is named a “signature mechanism giving message recovery” (see ISO/IEC 9796 (all parts)).

NOTE Any signature mechanism giving message recovery, for example, the mechanisms specified in ISO/IEC 9796 (all parts), can be converted to give a digital signature with appendix. This can be achieved by applying the signature mechanism to a hash-code derived as a function of the message. If this approach is employed, then all parties generating and verifying signatures must agree on this approach, and must also have a means of unambiguously identifying the hash-function to be used to generate the hash-code from the message.

The mechanisms specified in ISO/IEC 9796 (all parts) give either total or partial recovery, with the objective of reducing storage and transmission overhead. If the message is short enough, then the entire message can be included in the signature, and recovered from the signature in the verification process. Otherwise, a part of the message can be included in the signature, and the remainder stored and/or transmitted along with the signature.

The mechanisms specified in this part of ISO/IEC 9796 use a hash-function for hashing the entire message (possibly in more than one part). ISO/IEC 10118 specifies hash-functions for digital signatures.

Patent information

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 9796 may involve the use of a patent concerning the “Probabilistic signature scheme” (U.S. Patent 6,266,771 issued 2001-07-24).

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applications throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

University of California
Senior Licensing Officer
Office of Technology Transfer
1111 Franklin Street, 5th Floor
Oakland, California 94607-5200
USA

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 9796 may be the subject of patent rights other than that identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Security techniques — Digital signature schemes giving message recovery —

Part 2:
Integer factorization based mechanisms

1 Scope

This part of ISO/IEC 9796 specifies three digital signature schemes giving message recovery, two of which are deterministic (non-randomized) and one of which is randomized. The security of all three schemes is based on the difficulty of factorizing large numbers. All three schemes can provide either total or partial message recovery.

The method for key production for the three signature schemes is specified in this part of ISO/IEC 9796. However, techniques for key management and for random number generation (as required for the randomized signature scheme), are outside the scope of this part of ISO/IEC 9796.

Users of this standard are, wherever possible, recommended to adopt the second mechanism (Digital signature scheme 2). However, in environments where generation of random variables by the signer is deemed infeasible, then Digital signature scheme 3 is recommended. Digital signature scheme 1 shall only be used in environments where compatibility is required with systems implementing the first edition of this standard. However, Digital signature scheme 1 is only compatible with systems implementing the first edition of this standard that use hash-codes of at least 160 bits.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9796. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 9796 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9796-3:2000, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*

ISO/IEC 9797-2, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*

ISO/IEC 9798-1:1997, *Information technology – Security techniques – Entity authentication – Part 1: General*

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

ISO/IEC 14888 (all parts), *Information technology – Security techniques – Digital signatures with appendix*