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*

3 Terms and definitions

For the purposes of this part of ISO 9796, the following terms and definitions apply.

3.1
capacity
positive integer indicating the number of bits available within the signature for the recoverable part of the message.

3.2
certificate domain
collection of entities using public key certificates created by a single Certification Authority (CA) or a collection of CAs operating under a single security policy.

3.3
certificate domain parameters
cryptographic parameters specific to a certificate domain and which are known and agreed by all members of the certificate domain.

3.4
collision-resistant hash-function
hash-function satisfying the following property:
— it is computationally infeasible to find any two distinct inputs which map to the same output.
[ISO/IEC 10118-1: 2000]

3.5
hash-code
string of bits which is the output of a hash-function.
[ISO/IEC 10118-1: 2000]

3.6
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties
— for a given output, it is computationally infeasible to find an input which maps to this output;
— for a given input, it is computationally infeasible to find a second input which maps to the same output.
[ISO/IEC 9797-2: 2001]

3.7
mask generation function
function which maps strings of bits to strings of bits of arbitrary specified length, satisfying the following property
— it is computationally infeasible to predict, given one part of an output but not the input, another part of the output.

3.8
message
string of bits of any length.
[ISO/IEC 14888-1: 1998]

3.9
message representative
bit string derived as a function of the message and which is combined with the private signature key to yield the signature.

3.10
nibble
block of four consecutive bits (half an octet).

3.11
non-recoverable part
part of the message stored or transmitted along with the signature; empty when message recovery is total.

3.12
octet
string of eight bits.

3.13
private key
that key of an entity's asymmetric key pair which should only be used by that entity.
[ISO/IEC 9798-1: 1997]

3.14
private signature key
private key which defines the private signature transformation.
[ISO/IEC 9798-1: 1997]

3.15
public key
that key of an entity's asymmetric key pair which can be made public.
[ISO/IEC 9798-1: 1997]

3.16
public key system (for digital signature)
cryptographic scheme consisting of three functions:
- *Key production*, a method for generating a key pair made up of a private signature key and a public verification key,
- *Signature production*, a method for generating a signature Σ from a message representative F and a private signature key, and
- *Signature opening*, a method for obtaining the recovered message representative F^* from a signature Σ and a public verification key. The output of this function also contains an indication as to whether the signature opening procedure succeeded or failed.

3.17
public verification key
public key which defines the public verification transformation.
[ISO/IEC 9798-1: 1997]

3.18
recoverable part
part of the message conveyed in the signature.

3.19
salt
random data item produced by the signing entity during the generation of the message representative in Signature scheme 2.

3.20
signature
string of bits resulting from the signature process.
[ISO/IEC 14888-1: 1998]

3.21
trailer
string of bits of length one or two octets, concatenated to the end of the recoverable part of the message during message representative production.

4 Symbols and abbreviated terms

For the purposes of this part of ISO/IEC 9796, the following symbols and abbreviations apply.

NOTE – In most cases upper case letters are used to represent bit strings and octet strings, whereas lower case letters are used to represent functions.

C Octet string encoding the bit length of the recoverable part of the message (used in message representative production in Signature schemes 2 and 3).

c The capacity of the signature scheme, i.e. the maximum number of bits available for the recoverable part of the message.

c^* The recoverable message length, i.e. the length in bits of the recoverable part of the message ($c \geq c^*$).

D, D' Bit strings constructed during message representative production in Signature schemes 2 and 3.

D^*, D'^* Bit strings constructed during message recovery in Signature schemes 2 and 3.

F Message representative (a bit string).

F^* Recovered message representative (as output from the Signature opening step).

g Mask generation function.

H Hash-code computed as a function of the message M (a bit string).

H^* Recovered hash-code as derived during the Message recovery step.

h Collision-resistant hash-function.

k The bit length of the modulus of the private signature key and public verification key (see Annex A).

L_h The bit length of hash-codes produced by the hash-function h.

L_S The bit length of the salt S.

M Message to be signed (a bit string).

M^* Message recovered from a signature as a result of the verification process.

M_1 Recoverable part of the message M, i.e. $M = M_1||M_2$.

M_1^* Recovered recoverable part of the message (as generated during message recovery).

M_2 Non-recoverable part of the message M, i.e. $M = M_1||M_2$.

M_2^* Non-recoverable part of the message, as input to the verification process.

N Bit string constructed during message representative production in Signature schemes 2 and 3.

N^* Bit string generated during message recovery in Signature schemes 2 and 3.

P A string of zero bits constructed during message representative production in Signature schemes 2 and 3.

S Salt (a bit string).

S^* Recovered salt (a bit string).

t The number of octets in the Trailer field (t = 1 or 2).

T The Trailer field (a string of $8t$ bits used during message representative production).

Δ Integer in the range 0 to 7 used in the specification of message allocation.

δ Integer in the range 0 to 7 used in the specification of Signature schemes 2 and 3.

Σ Signature (a bit string containing k-1 or k bits).

$|A|$ The bit length of the bit-string A, i.e. the number of bits in A.

$A \,||\, B$ Concatenation of bit strings A and B (in that order).

$\lceil a \rceil$ for a real number a, the smallest integer not less than a.

a mod *n* for integers *a* and *n*, (*a* mod *n*) denotes the (non-negative) remainder obtained when *a* is divided by *n*. Equivalently if $b = a \bmod n$, then *b* is the unique integer satisfying:

(i) $0 \le b < n$, and

(ii) $(b-a)$ is an integer multiple of *n*.

5 Converting between bit strings and integers

To represent a non-negative integer *x* as a bit string of length *l* (*l* has to be such that $2^l > x$), the integer shall be written in its unique binary representation:

$$x = 2^{l-1}x_{l-1} + 2^{l-2}x_{l-2} + \ldots + 2x_1 + x_0$$

where $0 \le x_i < 2$ (note that one or more leading digits will be zero if $x < 2^{l-1}$). The bit string shall be

$$x_{l-1}\, x_{l-2} \ldots x_0.$$

To represent a bit string $x_{l-1}\, x_{l-2} \ldots x_0$ (of length *l*) as an integer *x*, the inverse process shall be followed, i.e. *x* shall be the integer defined by

$$x = 2^{l-1}x_{l-1} + 2^{l-2}x_{l-2} + \ldots + 2x_1 + x_0.$$

6 Requirements

Users who wish to employ a digital signature mechanism compliant with this part of ISO/IEC 9796 shall ensure that the following properties hold.

a) The message *M* to be signed shall be a binary string of any length, possibly empty.

b) The signature function uses a private signature key, while the verification function uses the corresponding public verification key.

- Each signing entity shall use and keep secret its private signature key corresponding to its public verification key.
- Each verifying entity should know the public verification key of the signing entity.

c) Use of the signature schemes specified in this standard requires the selection of a collision-resistant hash-function *h*. There shall be a binding between the signature mechanism and the hash-function in use. Without such a binding, an adversary might claim the use of a weak hash-function (and not the actual one) and thereby forge a signature.

NOTE 1 There are various ways to accomplish this binding. The following options are listed in order of increasing risk.

1. Require a particular hash-function when using a particular signature mechanism. The verification process shall exclusively use that particular hash-function. ISO/IEC 14888-3 gives an example of this option where the DSA mechanism requires the use of Dedicated Hash-function 3 from ISO/IEC 10118-3 (otherwise known as SHA-1).

2. Allow a set of hash-functions and explicitly indicate the hash-function in use in the certificate domain parameters. Inside the certificate domain, the verification process shall exclusively use the hash-function indicated in the certificate. Outside the certificate domain, there is a risk arising from certification authorities (CAs) that may not adhere to the user's policy. If, for example, an external CA creates a certificate permitting other hash-functions, then signature forgery problems may arise. In such a case a misled verifier may be in dispute with the CA that produced the other certificate.

3. Allow a set of hash-functions and indicate the hash-function in use by some other method, e.g., an indication in the message or a bilateral agreement. The verification process shall exclusively use the hash-function indicated by the other method. However, there is a risk that an adversary may forge a signature using another hash-function.

NOTE 2 The 'other method' referred to in paragraph 3 immediately above could be in the form of a hash-function identifier included in the message representative *F* (see clauses 8.1.2 and 9.1.3). If the hash-function identifier is included in *F* in this way then an attacker cannot fraudulently reuse an existing signature with the same M_1 and a different M_2, even when

the verifier could be persuaded to accept signatures created using a hash-function sufficiently weak that pre-images can be found. However, as discussed in detail in [11] (see also Annex C), in this latter case and using the weak hash-function, an attacker can still find a new signature with a 'random' M_1.

NOTE 3 The attack mentioned in Note 2 that yields a new signature with a 'random' M_1 can be prevented by requiring the presence of a specific structure in M_1. For instance, one may impose a length limit on M_1 that is sufficiently less than the capacity of the signature scheme (see Annex C for further discussion). For digital signature schemes 2 and 3, a length limit on M_1 may also prevent an attacker from reusing existing signatures even if no hash-function identifier is included in the message representative, provided that the mask generation function g is based on the hash-function. This holds under the reasonable assumption that the weak hash-function involved is a 'general purpose' hash-function, not one designed solely for the purpose of forging a signature.

The user of a digital signature mechanism should conduct a risk assessment considering the costs and benefits of the various alternative means of accomplishing the required binding. This assessment should include an assessment of the cost associated with the possibility of a bogus signature being produced.

d) The verifier of a signature shall always have a secure independent means of determining which of the three signature schemes specified in this standard have been employed to generate the signature. In addition, if Digital signature scheme 2 or 3 is being used, the signature verifier shall also have a means of determining which of the two signature production functions specified in Annex A have been used. This could, for example, be achieved by specifying the mechanism and signature production function in agreed 'domain parameters' or by including an unambiguous identifier for the signature scheme and signature production function in the signer's public key certificate. The signature production function may also be specified in an algorithm identifier associated with the signed data.

e) The digital signature schemes specified in this part of ISO/IEC 9796 each have particular options, the range of possible choices of which by the signer must be known to the verifier by a secure independent means. These options are as follows.

– For all three digital signature schemes, the verifier must know whether trailer field option 1 or 2 is being employed.

– For digital signature schemes 2 and 3, the verifier must know L_S, the length of the salt S.

This could, for example, be achieved by specifying the option selection in the 'domain parameters' or by including option information in the signer's public key certificate.

7 Model for signature and verification processes

The model for a signature scheme giving message recovery presented here applies to all three of the schemes in this part of ISO/IEC 9796. When applied to a message M, a signature scheme of this type can provide either total or partial message recovery.

- If M is sufficiently short, then message recovery can be total because it is possible for M to be entirely included in the signature.

- If M is too long, then message recovery will be partial. In this case M shall be divided into the *recoverable part*, a string of bits of limited length to be included in the signature, and the *non-recoverable part*, a string of octets of any length to be stored and/or transmitted along with the signature.

The model is divided into three parts: a specification of the procedure for signing a message, a specification of the procedure for verifying a signature, and details of the additional aspects of signing and verifying that need to be defined in order to complete the specification of a signature scheme. Clauses 8, 9 and 10 specify these additional aspects for the three schemes defined in this part of ISO/IEC 9796.

7.1 Signing a message

7.1.1 Overview

Given a message M to be signed, three steps need to be performed to generate a signature on M, namely message allocation, recoverable string production, and signature production.

- *Message allocation* consists of the process whereby the message is divided into two parts: a recoverable part M_1 and a non-recoverable part M_2 (which may be empty). The length of the recoverable part is bounded above by the capacity c of the signature scheme, a value determined by the choice of the signature scheme and the key for the scheme. The recoverable part will be recovered from the signature during the verification process, whereas the non-recoverable part must be made available to the verifier by other means (e.g. it can be sent or stored with the signature). Hence, if the message is sufficiently short, the entire message can be allocated to the recoverable part, and the non-recoverable part will be empty.

- *Message representative production* takes as input the two parts of the message, and outputs a formatted string, known as the *message representative*, which is input to the signature production step.

- *Signature production* takes as input the message representative and the private signature key and outputs the *signature* Σ. This process is performed using a public key system.

7.1.2 Message allocation

The choice of signature scheme and key for the scheme determine the capacity c of the signature, where c must satisfy $c \geq 7$. The message M to be signed shall be divided into two parts, M_1 and M_2, as follows.

A recoverable message length c^* shall be chosen, where $c^* \leq c$, $c^* \leq |M|$, and $c^* \equiv |M| \pmod 8$. For Signature scheme 1, c^* shall be set equal to the minimum of $c-\Delta$ and $|M|$, where $\Delta = (c-|M|) \bmod 8$.

- If $|M| = c^*$ then the entire message shall be recoverable, i.e. $M_1 = M$ and M_2 shall be empty.

- If $|M| > c^*$ then M_1 shall be set equal to the left-most c^* bits of M, and M_2 shall be set equal to the remainder of M, i.e. M_2 contains $|M|-c^*$ bits.

In either case it follows that $M = M_1||M_2$.

NOTE 1 For practical purposes, an application may wish to structure the message M to ensure that data it wants to be explicitly stored or transmitted (e.g., address information) is allocated to the non-recoverable message part M_2. However, the structure and interpretation of the message M are outside the scope of this part of ISO/IEC 9796.

NOTE 2 The method for message allocation ensures that M_2 is always a whole number of octets in length. Moreover, choosing c^* to be the minimum of $c-\Delta$ and $|M|$, where $\Delta = (c-|M|) \bmod 8$, ensures that M_1 is as long as possible subject to this constraint. Also, if M is a whole number of octets in length, i.e. if $|M|$ is an integer multiple of 8, then both M_1 and M_2 will consist of a whole number of octets.

7.1.3 Message representative production

This step takes as input the recoverable and non-recoverable parts of the message, M_1 and M_2, and outputs the message representative F. This shall be achieved using one of the methods specified in clauses 8, 9 and 10 of this part of ISO/IEC 9796. These methods require use of a hash-function h and, in the cases of the second and third mechanisms, a mask generation function g that also uses h. The hash-function h to be used shall be selected from amongst those standardised in ISO/IEC 10118; the mask generation function g shall be set equal to the function specified in Annex B of this part of ISO/IEC 9796.

7.1.4 Signature production

This step takes as input the message representative F and the private signature key and outputs the *signature* Σ. This shall be achieved using the public key system specified in Annex A to this part of ISO/IEC 9796.