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

Part 2:
Mechanisms using a hash-function

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

Partie 2: Mécanismes utilisant une fonction de hachage



Contents	Page
Foreword	iii
Introduction	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Symbols and abbreviations	3
5 Requirements	3
6 Signature process	4
7 Verification process	6

Annexes

A Example of a public-key system for digital signature	7
B Illustrative examples related to annex A	9

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. 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 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: *Mechanisms using a hash-function*

International Standard ISO/IEC 9796-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*.

Annexes A and B of this part of ISO/IEC 9796 are for information only.

Introduction

Digital signatures can be used to provide the electronic equivalent of a hand-written signature, for implementing services such as message authentication, message integrity and non-repudiation. These services apply to digital messages which are strings of bits, e.g., concatenations of data elements or concatenations of data objects.

Most digital signature schemes are based upon a particular public-key system. Any public-key system includes three basic operations:

- a process producing pairs of keys, a private key and a public key,
- a process using a private key,
- a process using a public key.

In any public-key digital signature scheme, the private key is used in a signature process for signing messages; the public key is used in a verification process for verifying signed messages. A pair of signature keys thus consists of a "private signature key" and a "public verification key".

There are two types of digital signature schemes.

- When the whole message or a part of the message may be recovered from the signature, the scheme is named a "digital signature scheme giving message recovery" (see ISO/IEC 9796).
- When the whole message has to be stored and transmitted along with the signature, the scheme is named a "digital signature scheme with appendix" (see ISO/IEC 14888).

NOTE — The two types of schemes are not mutually exclusive. Specifically, any scheme giving message recovery, e.g., ISO/IEC 9796:1991, can be used for provision of digital signatures with appendix. In this case, the signature is produced by applying the scheme to a hash-code computed from the message.

ISO/IEC 9796 specifies digital signature schemes giving either total or partial message recovery. One practical advantage of such schemes is that, depending upon the implementation environment, they may reduce data storage and transmission costs.

ISO/IEC 9796:1991 will be transformed into part 1. It specifies a digital signature scheme for messages of limited length, so that the message is completely recovered from the signature. The scheme does not involve a hash-function; it is designed so that, depending on the choice of parameters, the verification process can be extremely efficient, i.e., it can be implemented in environments with very limited processing capabilities.

This part of ISO/IEC 9796 uses a hash-function for hashing the entire message. If the message is short enough, then the verification process recovers the entire message and the hash-code from the signature. Otherwise, the verification process recovers only a part of the message along with the hash-code.

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

Part 2: Mechanisms using a hash-function

1 Scope

This part of ISO/IEC 9796 specifies a digital signature scheme for messages of any length. The messages are arbitrary strings of bits; no assumption is made as to the possible presence of natural redundancy.

The scheme uses a hash-function and a public-key system. It includes

- a signature process using successively a hash-function, format mechanisms and a signature function for signing messages,
- a verification process using successively a verification function, recovery mechanisms and a hash-function for checking signed messages.

The input to the signature function includes both the hash-code and all or part of the message. The verification function yields as an output the values input to the signature function. By this means, the scheme provides either total or partial message recovery.

This part of ISO/IEC 9796 does not specify the hash-function to be used. ISO/IEC 10118 specifies hash-functions appropriate for digital signatures.

This part of ISO/IEC 9796 does not specify the public-key system used to construct the signature and verification functions. Annex A gives an example of a suitable public-key system, including a key production process, a signature function and a verification function; this public-key system is currently the only one known appropriate for this part of ISO/IEC 9796. Annex B provides illustrative examples related to the operations specified in annex A.

Some parameters affect the security of the scheme. This part of ISO/IEC 9796 does not specify the values to be used to reach a given level of security; however, it is specified in such a way as to minimize the required changes in its use if some of these parameters need to be modified.

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 9796:1991, *Information technology — Security techniques — Digital signature scheme giving message recovery*.

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)¹⁾, *Information technology — Security techniques — Digital signatures with appendix*.

¹⁾ To be published.

3 Terms and definitions

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

3.1 keys

3.1.1

private signature key

private key which defines the private signature transformation

[ISO/IEC 9798-1:1997, definition 3.3.18]

3.1.2

public verification key

public key which defines the public verification transformation

[ISO/IEC 9798-1:1997, definition 3.3.23]

3.2

hash-function

function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties

- It is computationally infeasible to find for a given output an input which maps to this output.
- It is computationally infeasible to find for a given input a second input which maps to the same output.

[ISO/IEC 10118-1:1994, definition 2.4]

3.2.1

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 10118-1:1994, definition 2.1]

3.3 strings of bits

3.3.1

message

string of bits of any length, possibly empty

NOTE — Adapted from ISO/IEC 9796:1991, definition 2.1.

3.3.1.1

non-recoverable part

part of the message stored and transmitted along with the signature, empty when the recovery is total

3.3.1.2

recoverable part

part of the message conveyed in the signature, empty when the message itself is empty

3.3.2

intermediate string

string of bits from which the recoverable string is derived

3.3.2.1

header

leftmost field of the intermediate string (see table 1)

3.3.2.2

more-data bit

specific bit of the intermediate string, indicating whether the recovery is total or partial (see table 1)

3.3.2.3

padding field

field of the intermediate string, conveying the padding bits (see table 1)

3.3.2.3.1

border bit

rightmost bit of the padding field

3.3.2.4

data field

field of the intermediate string, conveying the recoverable part (see table 1)

3.3.2.5

hash field

field of the intermediate string, conveying the hash-code (see table 1)

3.3.2.6

trailer

rightmost field of the intermediate string (see table 1)

3.3.2.6.1

hash-function identifier

optional byte of the trailer, identifying a hash-function

3.3.3

nibble

block of four consecutive bits

3.3.3.1

border nibble

specific nibble of the intermediate string, containing the border bit

3.3.4

recoverable string

string of bits derived from the intermediate string, input to the signature function

3.3.5

signature

string of bits resulting from the signature process

[ISO/IEC 9796:1991, definition 2.2]

3.3.6 coding conventions

3.3.6.1

bit numbering

In all strings of x bits, the numbering starts from the rightmost bit b_1 (the last bit) to the leftmost bit b_x (the first bit).

3.3.6.2

bit significance

All integers are written with the most significant digit (or bit or nibble or byte) in the leftmost position.

NOTE — For example, for computing a byte value, b_1 is the least significant bit and b_8 is the most significant bit.