

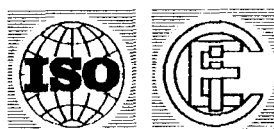
INTERNATIONAL STANDARD

ISO/IEC
9796

First edition
1991-09-15

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

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



Reference number
ISO/IEC 9796:1991(E)



Documents

Document Sharing Hub

Contents

	Page
Foreword	iii
Introduction	iv
1 Scope	1
2 Definitions	1
3 Symbols and abbreviations	1
4 General overview	1
5 Signature process	2
6 Verification process	3

Annexes

A Example of a public-key system for digital signature	4
B Illustrative examples related to annex A	6
C Some precautions taken against various potential attacks related to annex A	11
D Bibliography	12

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.

International Standard ISO/IEC 9796 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Annexes A, B, C and D are for information only.

Introduction

A digital signature in electronic exchange of information is a counterpart to a handwritten signature in classical mail.

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 secret key and a public key ;
- a process using a secret key ;
- a process using a public key.

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

Two types of digital signature schemes are clearly identified.

- When the verification process needs the message as part of the input, the scheme is named a "signature scheme with appendix". The use of a hash-function is involved in the calculation of the appendix.
- When the verification process reveals the message together with its specific redundancy (sometimes called the "shadow of a message"), the scheme is named a "signature scheme giving message recovery".

This International Standard specifies a scheme for digital signature of messages of limited length.

This digital signature scheme allows a minimal resource requirement for verification. It does not involve the use of a hash-function and it avoids the known attacks against the generic algorithm in use.

The message need not be in a natural language. It may be any arbitrary string of bits of limited length. Examples of such messages are cryptographic key materials and the result of hashing another, longer message, which is also called the "imprint of a message". A characteristic example is a structured set of a few strings of bits generated by cryptographic software and hardware, one of these strings coding control information produced within the hardware.

NOTE — The use of this International Standard may involve patented items.

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

1 Scope

This International Standard specifies a digital signature scheme giving message recovery for messages of limited length and using a public-key system.

This digital signature scheme includes

- a signature process using a secret signature key and a signature function for signing messages;
- a verification process using a public verification key and a verification function for checking signatures while recovering messages.

During the signature process, messages to be signed are padded and extended if necessary. Artificial redundancy is then added, depending upon the message itself. No assumption is made as to the possible presence of natural redundancy in the messages. The artificial redundancy is revealed by the verification process. The removal of this artificial redundancy gives message recovery.

This International Standard does not specify the key production process, the signature function and the verification function. Annex A gives an example of a public-key system including key production, signature function and verification function. The various steps of these operations are illustrated by examples in annex B.

Some parameters in the scheme are related to security: this International Standard does not specify the values to be used in order to reach a given level of security. However, this International Standard is specified in such a way as to minimize the required changes in its use if some of these parameters have to be modified.

2 Definitions

For the purposes of this International Standard, the following definitions apply.

- 2.1 message:** String of bits of limited length.
- 2.2 signature:** String of bits resulting from the signature process.

3 Symbols and abbreviations

<i>MP</i>	Padded message
<i>ME</i>	Extended message
<i>MR</i>	Extended message with redundancy
<i>IR</i>	Intermediate integer
Σ	Signature
k_s	Length of the signature in bits
<i>IR'</i>	Recovered intermediate integer
<i>MR'</i>	Recovered message with redundancy
<i>MP'</i>	Recovered padded message
Sign	Signature function under control of the secret signature key
Verif	Verification function under control of the public verification key
mod <i>z</i>	Arithmetic computation modulo <i>z</i>
μ	Nibble
<i>II</i>	Permutation of the nibbles
<i>m</i>	Byte
<i>S</i>	Shadow of the bytes
<i>X</i> <i>Y</i>	Concatenation of strings of bits <i>X</i> and <i>Y</i>
<i>X</i> ⊕ <i>Y</i>	Exclusive-or of strings of bits <i>X</i> and <i>Y</i>

NOTES

- 1 All integers (and all strings of bits or bytes) are written with the most significant digit (or bit or byte) in left position.
- 2 The hexadecimal notation, with the digits 0 to 9 and A to F, is used in table 1 and in annex B.

4 General overview

- The next two clauses specify
- the signature process in clause 5;
 - the verification process in clause 6.

Each signing entity shall use and keep secret its own signature key corresponding to its own public verification key.

Messages to be signed shall be padded and extended if necessary. Redundancy is then added according to rules specified in clause 5. From the extended messages with redundancy, signatures shall be computed using the secret signature key as specified in clause 5.

Each verifying entity should know and use the public verification key specific to the signing entity. A signature shall be accepted if and only if the verification process specified in clause 6 is successful.

NOTE — The production and the distribution of keys fall outside the scope of this International Standard.

5 Signature process

Figure 1 summarizes the signature process.

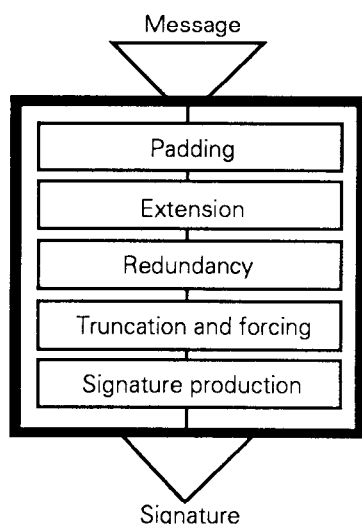


Figure 1 — Signature process

NOTE — A good implementation of the signature process should physically protect the operations in such a way that there is no direct access to the signature function under control of the secret signature key.

5.1 Padding

The message is a string of bits. This string of bits is padded to the left by 0 to 7 zeroes so as to obtain a string of z bytes. Index r , to be used later on, is the number of padded zeroes plus one. Index r is thus valued from 1 to 8.

Consequently, in the padded message denoted by MP , the $8z+1-r$ least significant bits are information bearing.

$$MP = m_z \parallel m_{z-1} \parallel \dots \parallel m_2 \parallel m_1$$

$$m_z = (r-1 \text{ padded zeroes}) \parallel (9-r \text{ information bits})$$

Number z multiplied by sixteen shall be less than or equal to number k_s+3 . Consequently, the number of bits of the message to be signed shall be at most 8 times the largest integer less than or equal to $(k_s+3)/16$.

5.2 Extension

Number t , to be used later on, is the least integer such that a string of $2t$ bytes includes at least k_s-1 bits.

The extended message ME is obtained by repeating the z bytes of MP , as many times as necessary, in order and concatenated to the left, until forming a string of t bytes.

For i valued from 1 to t and j equal to $i-1 \pmod{z}$ plus one (j is therefore valued from 1 to z), the i -th byte of ME equals the j -th byte of MP .

$$ME = \dots m_z \parallel \dots m_2 \parallel m_1$$

<----- t bytes ----->

NOTE — Number z is less than or equal to number t . The equality may occur only if k_s is congruent to 13, 14, 15, 0 or 1 mod 16.

5.3 Redundancy

The extended message with redundancy MR is obtained by interleaving the t bytes of ME in odd positions and t bytes of redundancy in even positions. Altered by index r , the least significant nibble of the $2z$ -th byte of MR codes the message length by its value and its position.

For i valued from 1 to t ,

— the $(2i-1)$ -th byte of MR equals the i -th byte of ME ;

— the $2i$ -th byte of MR equals the image of the i -th byte of ME according to the shadow S specified in table 1, except for the $2z$ -th byte of MR which equals the exclusive-or of index r with the shadow of the z -th byte of ME .

$$MR = \dots S(m_z) \oplus r \parallel m_z \parallel \dots S(m_2) \parallel m_2 \parallel S(m_1) \parallel m_1$$

<----- $2t$ bytes ----->

NOTE — The computation of the $2t$ bytes of MR (mr_{2t} to mr_1) from the z bytes of MP (mp_z to mp_1) is performed by applying successively the following three formulae for i valued from 1 to t .

$$j := (i-1 \pmod{z}) + 1; \quad mr_{2i-1} := mp_j; \quad mr_{2i} := S(mp_j)$$

Finally, the $2z$ -th byte is altered by index r .

$$mr_{2z} := r \oplus mr_{2z}$$

5.4 Truncation and forcing

The intermediate integer IR is coded by a string of k_s bits where the most significant bit is valued to 1 and where the k_s-1 least significant bits are those of MR , except for the least significant byte which is replaced. If $\mu_2 \parallel \mu_1$ is the least significant byte of MR , then the least significant byte of IR shall be $\mu_1 \parallel 6$.

5.5 Signature production

The signature Σ is obtained as a string of k_s bits by applying to IR the signature function under control of the secret signature key.

$$\Sigma = \text{Sign}(IR)$$