INTERNATIONAL STANDARD

ISO/IEC 9796-3

Second edition
2006-09-15

Corrected version
2013-09-15

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

Part 3: Discrete logarithm based mechanisms

Technologies de l'information — Techniques des sécurité — Schémas de signature numérique rétablissant le message —
Partie 3: Mécanismes basés sur les logarithmes discrets

Reference number
ISO/IEC 9796-3:2006(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

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 9796-3 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 9796-3:2000), which has been technically revised. New mechanisms and object identifiers have been specified.

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

— *Part 2: Integer factorization based mechanisms*

— *Part 3: Discrete logarithm based mechanisms*

This corrected version of ISO/IEC 9796-3:2006 incorporates the following corrections:

— The year of publication has been removed from references to ISO/IEC 15946-1.

— The last paragraph of 6.2.1 has been modified and ISO/IEC 15946-5 has been added to Clause 2.

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 only the public verification key and not the private signature key, it is computationally infeasible to produce a valid signature for any given message;

— the signatures produced by a signer can neither be used for producing a valid signature for any new message nor for recovering the signature key;

— it is computationally infeasible, even for the signer, to find two different messages with the same signature.

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 using the private signature key, called the ***signature generation process***;

— a process using the public verification key, called the ***signature verification process***.

There are two types of digital signature mechanisms:

— when, for each given private signature key, the signatures produced for the same message are the same, the mechanism is said to be ***non-randomized*** (or ***deterministic***) [see ISO/IEC 14888-1];

— when, for a given message and a given private signature key, each application of the signature process produces a different signature, the mechanism is said to be ***randomized***.

This part of ISO/IEC 9796 specifies randomized mechanisms.

Digital signature schemes 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 a part of it is recovered from the signature, the mechanism is named a ***signature mechanism giving message recovery***.

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

This part of ISO/IEC 9796 includes six mechanisms, one of which was in ISO/IEC 9796-3:2000 and five of which are in ISO/IEC 15946-4:2004. The mechanisms specified in this part of ISO/IEC 9796 use a hash-function to hash the entire message. ISO/IEC 10118 specifies hash-functions. Some of the mechanisms specified in this part of ISO/IEC 9796 use a group on an elliptic curve over finite field. ISO/IEC 15946-1 describes the mathematical background and general techniques necessary for implementing cryptosystems based on elliptic curves defined over finite fields.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the mechanisms NR, ECMR and ECAO given in Clause 8, 10 and 11, respectively.

Area	Patent no.	Issue date	Inventors
NR [see Clause 8]	US 5 600 725, EP 0 639 907	1997-02-04	K. Nyberg and R. A. Rueppel
ECMR [see Clause 10]	JP H09-160492 (patent application)		A. Miyaji
ECAO [see Clause 11]	JP 3 434 251	2003-08-04	M. Abe and T. Okamoto

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

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

Patent no.	Name of holder of patent right	Contact address
US 5 600 725, EP 0 639 907	Certicom Corp.	5520 Explorer Drive, 4th Floor, Mississauga, Ontario, Canada L4W 5L1
JP H09-160492	Matsushita Electric Industrial Co., Ltd.	Matsushita IMP Building 19th Floor, 1-3-7, Sironi, Chuo-ku, Osaka 540-6319, Japan
JP 3 434 251	NTT Intellectual Property Center	9-11 Midori-Cho 3-chome, Musashino-shi, Tokyo 180-8585, Japan

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.

NOTE 1 Computational feasibility depends on the specific security requirements and environment.

NOTE 2 Any signature mechanism giving message recovery — for example, the mechanisms specified in this part of ISO/IEC 9796 — can be converted for provision of digital signatures with appendix. In this case, the signature is produced by application of the signature mechanism to a hash-token of the message.

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

Part 3: Discrete logarithm based mechanisms

1 Scope

This part of ISO/IEC 9796 specifies six digital signature schemes giving message recovery. The security of these schemes is based on the difficulty of the discrete logarithm problem, which is defined on a finite field or an elliptic curve over a finite field.

This part of ISO/IEC 9796 also defines an optional control field in the hash-token, which can provide added security to the signature.

This part of ISO/IEC 9796 specifies randomized mechanisms.

The mechanisms specified in this part of ISO/IEC 9796 give either total or partial message recovery.

NOTE For discrete logarithm based digital signature schemes with appendix, see ISO/IEC 14888-3.

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 15946-1, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*

ISO/IEC 15946-5, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
data input
octet string which depends on the entire message or a portion of the message and which forms a part of the input to the signature generation process

3.2
domain parameter
data item which is common to and known by or accessible to all entities within the domain

[ISO/IEC 14888-1:1998]

NOTE The set of domain parameters may contain data items such as hash-function identifier, length of the hash-token, maximum length of the recoverable part of the message, finite field parameters, elliptic curve parameters, or other parameters specifying the security policy in the domain.

3.3
elliptic curve
set of points $P = (x, y)$, where x and y are elements of an explicitly given finite field, that satisfy a cubic equation without any singular point, together with the "point at infinity" denoted by $\circ$

[ISO/IEC 15946-1:2002]

NOTE For a mathematical definition of an elliptic curve over an explicitly given finite field, see Clause A.4.

3.4
explicitly given finite field
set of all e-tuples over $[0, p-1]$, where p is prime and $e \geq 1$, along with a "multiplication table"

NOTE 1 For a mathematical definition of an explicitly given finite field, see Clause A.3.

NOTE 2 For more detailed information on finite fields, see ISO/IEC 15946-1.

3.5
hash-code
string of octets which is the output of a hash-function

NOTE Adapted from ISO/IEC 10118-1:2000.

3.6
hash-function
function which maps strings of octets to fixed-length strings of octets, 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.

NOTE 1 Adapted from ISO/IEC 10118-1:2000.

NOTE 2 Computational feasibility depends on the specific security requirements and environment.

NOTE 3 For the purposes of this part of ISO/IEC 9796, the allowable hash-functions are those described in ISO/IEC 10118-2 and ISO/IEC 10118-3, with the following proviso:

— The hash-functions described in ISO/IEC 10118 map bit strings to bit strings, whereas in this part of ISO/IEC 9796, they map octet strings to octet strings. Therefore, a hash-function in ISO/IEC 10118-2 or ISO/IEC 10118-3 is allowed in this part of ISO/IEC 9796 only if the length in bits of the output is a multiple of 8, in which case the mapping between octet strings and bit strings is affected by the functions OS2BSP and BS2OSP.

3.7
hash-token
concatenation of a hash-code and an optional control field which can be used to identify the hash-function and the padding method

[ISO/IEC 14888-1:1998]

NOTE The control field with the hash-function identifier is mandatory unless the hash-function is uniquely determined by the signature mechanism or by the domain parameters.

3.8
message
string of octets of any length

3.9
parameter generation process
process which gives as its output domain parameter and user keys

3.10
pre-signature
octet string computed in the signature generation process which is a function of the randomizer but which is independent of the message

NOTE Adapted from ISO/IEC 14888-1:1998.

3.11
private signature key
data item specific to an entity and usable only by this entity in the signature generation process

3.12
public verification key
data item which is mathematically related to a private signature key and is known by or accessible to all entities and which is used by the verifier in the signature verification process

3.13
randomized
dependent on a randomizer

[ISO/IEC 14888-1]

3.14
randomizer
secret integer produced by the signing entity in the pre-signature production process, and not predictable by other entities

NOTE Adapted from ISO/IEC 14888-1:1998.

3.15
signature
pair of an octet string and an integer for providing authentication, generated in the signature generation process

NOTE Adapted from ISO/IEC 14888-1:1998.

3.16
signature generation process
process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature

NOTE Adapted from the definition of **signature process** in ISO/IEC 14888-1:1998.

3.17
signature verification process
process, which takes as its input the signed message, the verification key and the domain parameters, and which gives as its output the recovered message if valid

NOTE Adapted from the definition of **verification process** in ISO/IEC 14888-1:2008.

3.18
signed message
set of data items consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field

[ISO/IEC 14888-1:1998]

3.19
user keys
data item of a set of private signature key and public verification key

4 Symbols, notation and conventions

4.1 Symbols and notation

For the purposes of this document, the following symbols and notation apply.

A	entity, usually signer
B	entity, usually verifier
d	data input (octet string)
d'	recovered data input (octet string)
E	elliptic curve over explicitly given finite field
F	explicitly given finite field
G	generator of underlying group (finite field element / elliptic curve point)
h	(truncated) hash-token (octet string)
h'	recovered (truncated) hash-token (octet string)
h''	recomputed (truncated) hash-token (octet string)
Hash, Hash_1, Hash_2	hash-function
k	randomizer (integer)
KDF	key derivation function (synonym for MGF)
L_{clr}	length in octets of non-recoverable part (integer)
L_{dat}	length in octets of data input (integer)
L_F	length in octets of explicitly given finite field F (non-negative integer)
L_{rec}	(maximum) length in octets of recoverable part (integer)
L_{red}	length in octets of (added) redundancy (integer)
$L(x)$	length in octets of integer x or octet string x (non-negative integer)
L_{Hash}	length in octets of output of hash-function Hash (non-negative integer)
M	message (octet string)
M_{clr}	non-recoverable part of message (octet string)
M_{rec}	recoverable part of message (octet string)
M'	recovered message (octet string)
M'_{clr}	received non-recoverable part of message (octet string)
M'_{rec}	recovered part of message (octet string)
MGF	mask generation function
n	order of group generated by G (prime number)

$\mathcal{O}$	point at infinity of elliptic curve
p	prime number
P	element dependent on the chosen key generation scheme, that is $P = G$ for Key Generation Scheme I and $P = Y_A$ for Key Generation Scheme II [see Clause 7.3]
Π	pre-signature (octet string)
Π'	recovered pre-signature (octet string)
q	prime power
Q	element dependent on the chosen key generation scheme, that is $Q = Y_A$ for Key Generation Scheme I and $Q = G$ for Key Generation Scheme II [see Clause 7.3]
r	first part of signature (octet string)
r'	first part of recovered signature (octet string)
s	second part of signature (integer)
s'	second part of recovered signature (integer)
x_A	private signature key of entity A
Y_A	public verification key of entity A
$\{0,1\}^*$	set of finite bit strings
$\{0,1\}^{8*}$	set of finite octet strings
$\{0,1\}^{\ell}$	set of bit strings of length ℓ, where ℓ is a non-negative integer
$\{0,1\}^{8\ell}$	set of octet strings of length ℓ, where ℓ is a non-negative integer
$[a, b]$	set of integers x satisfying $a \le x \le b$, where a and b are integers
$\lvert x \rvert$	length of bit string x
$\lvert X \rvert$	cardinality of set X
$[x]^{\ell}$	leftmost ℓ-bits of octet string x, appending zeros to the right when $8\ell > L(x)$
$[x]_{\ell}$	rightmost ℓ-bits of octet string x, appending zeros to the left when $8\ell > L(x)$
$x \bmod n$	$r \in [0, n-1]$ such that $(x - r)$ is divisible by n, where x is an integer
$x \oplus y$	bitwise exclusive-OR operation of bit strings x and y
$x \lVert y$	concatenation of bit strings x and y
$X \times Y$	Cartesian product of sets X and Y

4.2 Conversion functions and mask generation functions

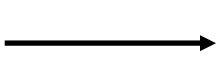
For the purposes of this document, the following conversion functions and mask generation functions are used.

BS2IP	bit-string-to-integer primitive [see Clause B.2]
BS2OSP	bit-string-to-octet-string primitive [see Clause B.1]
EC2OSP	elliptic-curve-to-octet-string primitive [see Clause B.6]
FE2IP	finite-field-element-to-integer primitive [see Clause B.4]
FE2OSP	finite-field-element-to-octet-string primitive [see Clause B.5]
I2BSP	integer-to-bit-string primitive [see Clause B.2]
I2OSP	integer-to-octet-string primitive [see Clause B.3]
MGF1	mask generation function 1 [see Clause C.2]
MGF2	mask generation function 2 [see Clause C.3]
OS2BSP	octet-string-to-bit-string primitive [see Clause B.1]
OS2ECP	octet-string-to-elliptic-curve primitive [see Clause B.6]
OS2FEP	octet-string-to-finite-field-element primitive [see Clause B.5]
OS2IP	octet-string-to-integer primitive [see Clause B.3]

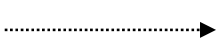
4.3 Legend for figures

The following legend is used for the figures in Clause 7 depicting the signature generation and verification processes for digital signatures giving message recovery.

step of the process



mandatory data flow



optional data flow

5 Binding between signature mechanisms and hash-functions

Use of the signature schemes specified in this part of ISO/IEC 9796 requires the selection of a hash-function Hash. ISO/IEC 10118 specifies hash-functions. 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.

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.

NOTE 1 One of the security requirements for the hash-function Hash used in this part of ISO/IEC 9796 is so-called "collision-resistance."

NOTE 2 There are various ways to accomplish this binding. The following options are listed in order of increasing risk:

a) 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 (otherwise known as SHA-1) from ISO/IEC 10118-3;

b) 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; and

c) 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 3 The "other method" referred to in paragraph c) immediately above could be in the form of a hash-function identifier included in the octet string representative d. If the hash-function identifier is included in d in this way then an attacker cannot fraudulently reuse an existing signature with the same octet string d_1 and a different d_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, in this latter case and using the weak hash-function, an attacker can still find a new signature with a "random" d_1.

NOTE 4 The attack mentioned in Note 3 that yields a new signature with a "random" d_1 can be prevented by requiring the presence of a specific structure in d_1. For instance, one may impose a length limit on d_1 that is sufficiently less than the capacity of the signature scheme. For some digital signature schemes, a length limit on d_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 MGF 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.

6 Framework for digital signatures giving message recovery

6.1 Processes

Clauses 6.2 through 6.4 contain a high-level description of a general model for the six signature schemes specified in this part of ISO/IEC 9796. A detailed description of the general model is provided in Clause 7.

A digital signature scheme specified in this part of ISO/IEC 9796 is defined by the specification of the following processes:

— parameter generation process;

— signature generation process;

— signature verification process.