INTERNATIONAL STANDARD

ISO/IEC 18370-2

First edition
2016-07-01

Information technology — Security techniques — Blind digital signatures —

Part 2: Discrete logarithm based mechanisms

Technologie de l'information — Techniques de sécurité — Signatures numériques en aveugle —
Partie 2: Mécanismes fondés sur le logarithme discret

Reference number
ISO/IEC 18370-2:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 18370 consists of the following parts, under the general title *Information technology — Security techniques — Blind digital signatures*:

— *Part 1: General*

— *Part 2: Discrete logarithm based mechanisms*

Further parts may follow.

Introduction

Blind digital signature mechanisms are a special type of digital signature mechanism, as specified in ISO/IEC 9796 (all parts) and ISO/IEC 14888, which allow a user (a requestor) to obtain a signature from a signer of the user's choice, without giving the signer any information about the message that is signed or the resulting signature.

In some mechanisms, the signer does not completely lose control over the signed message since the signer can include explicit information in the resulting signature under an agreement with the requestor. These types of blind signatures are called blind signatures with partial disclosure.

Other mechanisms allow a requestor to receive a blind signature on a message not known to the signer but the choice of the message is restricted and needs to conform to certain rules. Such mechanisms are called blind signature mechanisms with selective disclosure.

Depending on the mechanism, it may be possible for an authorized entity to trace a signature to the requestor who requested it. Such an entity can either identify a signature that resulted from a given signature request (signature tracing), or link a signature to the receiver who requested it (requestor tracing). Blind signature mechanisms with tracing features are called traceable blind signature mechanisms.

ISO/IEC 18370 specifies blind digital signature mechanisms, as well as three variants: blind digital signature mechanisms with partial disclosure, blind digital signature mechanisms with selective disclosure and traceable blind digital signature mechanisms. ISO/IEC 18370-1 specifies principles and requirements for these mechanisms. This part of ISO/IEC 18370 specifies several specific instances of these mechanisms.

The security of blind digital signature mechanisms and their variants depends on computational problems believed to be intractable, i.e. problems for which, given current knowledge, finding a solution is computationally infeasible, such as the integer factorization problem or the discrete logarithm problem in an appropriate group. The mechanisms specified in this part of ISO/IEC 18370 are based on the latter problem.

ISO/IEC 18370 does not specify mechanisms for key management or for certification of public keys. A variety of means are available for obtaining a reliable copy of the public verification key, e.g. a public key certificate. Techniques for managing keys and certificates are outside the scope of ISO/IEC 18370. For further information, see ISO/IEC 9594-8, ISO/IEC 11770-3 and ISO/IEC 15945.

This part of ISO/IEC 18370 specifies mechanisms that use a collision resistant hash-function to hash the message to be blindly signed. ISO/IEC 10118 specifies hash-functions.

The generation of key pairs requires random bits and prime numbers. The generation of signatures requires random bits. Techniques for producing random bits and prime numbers are outside the scope of ISO/IEC 18370. For further information, see ISO/IEC 18031 and ISO/IEC 18032.

Information technology — Security techniques — Blind digital signatures —

Part 2:
Discrete logarithm based mechanisms

1 Scope

This part of ISO/IEC 18370 specifies blind digital signature mechanisms, together with mechanisms for three variants of blind digital signatures. The variants are blind digital signature mechanisms with partial disclosure, blind digital signature mechanisms with selective disclosure and traceable blind digital signature mechanisms. The security of all the mechanisms in this part of ISO/IEC 18370 is based on the discrete logarithm problem.

For each mechanism, this part of ISO/IEC 18370 specifies the following:

— the process for generating the keys of the entities involved in these mechanisms;

— the process for producing blind signatures;

— the process for verifying signatures.

This part of ISO/IEC 18370 specifies another process specific to blind signature mechanisms with selective disclosure, namely, the following:

— the presentation process.

Furthermore, this part of ISO/IEC 18370 specifies other processes specific to traceable blind signature mechanisms, namely, the following:

a) the process for tracing requestors;

b) the process for tracing signatures;

c) the requestor tracing evidence evaluation process (optional);

d) the signature tracing evidence evaluation process (optional).

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18370-1 and the following apply.

3.1
abelian group
group $(G, *)$ such that $a * b = b * a$ for every a and b in G

3.2
cyclic group
group G of n elements that contains an element a in G, called the generator, of order n

[SOURCE: ISO/IEC 14888-3:2006, 3.2]

3.3
elliptic curve over a finite field
set E of points $P = (x, y)$, where x and y are elements of the *finite field* (3.6), that satisfy a certain equation, together with an extra point referred to as the point at infinity

Note 1 to entry: In this part of ISO/IEC 18370, only finite fields containing exactly q elements for a prime $q > 3$ are considered. In this case, the equation that every point $P = (x, y)$ of E (other than the point at infinity) should satisfy is of the form $y^2 = x^3 + ax + b$. The finite field elements a and b should satisfy $4a^3 + 27b^2 \neq 0_F$ (where 0_F is the additive identity element of the finite field).

Note 2 to entry: The set of points E, together with an appropriately defined operation, forms a *finite commutative group* (3.5), where the point at infinity is the identity element.

3.4
field
set of elements S and a pair of operations (+,*) defined on S, such that: i) $a * (b + c) = a * b + a * c$ for every a, b and c in S, ii) S together with + forms an *abelian group* (3.1) (with identity element 0), and iii) S excluding 0 together with * forms an abelian group

3.5
finite commutative group
abelian group (3.1) $(G, *)$ with a finite number of elements

Note 1 to entry: If $a^0 = e$, and $a^{n+1} = a * a^n$ (for $n \geq 0$) is defined recursively, the order of $a \in G$ is the least positive integer n, such that $a^n = e$.

Note 2 to entry: In some cases, such as when G is the set of points on an elliptic curve, arithmetic in the finite set G is described using additive notation.

3.6
finite field
field (3.4) such that the underlying set of elements is finite

Note 1 to entry: For any positive integer, m and a prime p, there exists a finite field containing exactly $q = p^m$ elements. This field is unique up to an isomorphism and is denoted by F_q.

[SOURCE: ISO/IEC 18033-2:2006, 3.21]

3.7
group
set of elements G and an operation * defined on the set of elements such that: i) $(a * b) * c = a * (b * c)$ for every a, b and c in G, ii) there exists an identity element, e in G, such that $a * e = e * a = a$ for every a in G, and iii) for every a in G, there exists an inverse element, a^{-1} in G, such that $a * a^{-1} = a^{-1} * a = e$

3.8
security parameters
variables that determine the security strength of a mechanism

4 Symbols

$a \in A$ indicates that element a is in set A

$a \| b$ concatenation of data items a and b in the order specified. In cases where the result of concatenating two or more data items is input to a cryptographic algorithm as part of one of the mechanisms specified in this part of ISO/IEC 18370, this result shall be composed so that it can be uniquely resolved into its constituent data strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property could be achieved in a variety of different ways, depending on the application. For example, it could be guaranteed by a) fixing the length of each of the substrings throughout the domain of use of the mechanism, or b) encoding the sequence of concatenated strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1[1].

$A \subseteq B$ indicates that the set A is a subset of or equal to set B

$A \setminus B$ when A and B are sets, this represents the set of elements present in A but not in B.

$|D|$ bit length of D if D is a bit string, or bit size of D if D is a non-negative number (i.e. 0 if $D = 0$, or the unique integer i such that $2^{i-1} \leq D < 2^i$ if $D > 0$).

E an elliptic curve over the finite field F_p, for a prime $p > 3$

$E(F_p)$ the set of all points (x, y), $x \in F_p$, $y \in F_p$, which satisfy the defining equation of the curve E, together with the point at infinity, O_E

$\#E(F_p)$ the order (or cardinality) of $E(F_p)$

F_p the finite field containing exactly p elements

g a generator of G_q

$gcd(N_1, N_2)$ the greatest common divisor of integers N_1 and N_2

G_q a cyclic group of prime order q. For uniformity, the multiplicative notation is used throughout. As such, when using the elliptic curve construction, it should be understood that ab represents the group addition of points a and b, that a/b represents the group addition of the point a to the additive inverse of the point b, and that a^b represents the scalar multiplication of point a by the integer b.

NOTE This part of ISO/IEC 18370 considers two constructions for the group G_q, in which it is infeasible to compute discrete logarithms. The first is based on a subgroup of a finite field, and the second is based on elliptic curves over a finite field F_q, where q is a prime number. Details of these two constructions are provided in Annex C.

H a cryptographic hash-function

I a set of integers

$[n]P$ scalar multiplication operation that takes a positive integer n and a point P on the elliptic curve E as input and produces as output another point Q on the elliptic curve E, where $Q = [n]P = P + P + ... + P$ added n - 1 times. The operation satisfies $[0]P = O_E$ (the point at infinity), and $[-n]P = [n](-P)$.

O_E the point at infinity on the elliptic curve E

$P + Q$ the elliptic curve sum of points P and Q

q a prime number satisfying $|q| = l_q$ where l_q is a security parameter

Z_p the set of integers in $[0, p - 1]$ with arithmetic defined modulo p

Z_N^* the set of integers U with $0 < U < N$ and $gcd(U, N) = 1$, with arithmetic defined modulo N

$\prod_{(i \in I)} a_i$ product of the values a_i for which $i \in I$

$[x, y]$ the set of integers from x to y inclusive, if x, y are integers satisfying $x \leq y$

$\langle \ldots \rangle$ an ordered list of values to be hashed

5 General requirements

In order to use any of the mechanisms specified in this part of ISO/IEC 18370, the following requirements shall be met.

— Each entity involved in a blind signature mechanism shall be aware of the public domain parameters.

— Each entity shall have access to an authentic copy of the necessary public keys, such as the public verification key.

— Each requestor in a traceable blind signature mechanism shall have a distinguishing identifier that is unambiguously bound to the private requestor key. The distinguishing identifier for a requestor can be the public requestor key.

— Both signer and requestor shall have the means to generate integers uniformly at random from a given range. Techniques for generation of sequences of random bits are specified in ISO/IEC 18031. A method for converting a string of bits to an integer in a given range is specified in Annex B.

— A collision-resistant hash-function such as one of those specified in ISO/IEC 10118 shall be used.

Before issuing a blind signature, the signer might wish to authenticate the requestor. ISO/IEC 18370 does not specify mechanisms for entity authentication. For this purpose, the use of one of the mechanisms specified in ISO/IEC 9798 is recommended.

For traceable blind signature mechanisms, this part of ISO/IEC 18370 does not specify in which circumstances a requestor tracing process or a signature tracing process is used.

6 Blind signature mechanisms

6.1 General

Clause 6 specifies a blind signature mechanism.

NOTE The mechanism in Clause 6 is based on Reference [23] and the associated security analysis is given in Reference [26].

6.2 Mechanism 1

6.2.1 Security parameters

The following symbols apply in the specification of this mechanism:

— k, l_q: security parameters.

The parties should agree on the security parameters in use. Guidance for parameter choice is given in Annex E.

6.2.2 Key generation process

The key generation process of a blind signature mechanism consists of the following procedures:

a) generating domain parameters;

b) generating a private signature key and a public verification key.

The first procedure is executed once when the domain is set up. The second procedure is executed for each signer within the domain, where the outputs are a private signature key and the corresponding public verification key.

The set of domain parameters includes the following parameters:

— q: a prime number where $|q| = l_q$;

— G_q: a cyclic group of prime order q;

— g_1: a random generator of G_q;

— g_2: a random generator of G_q different from g_1;

NOTE 1 An example of recommended parameters for typical security levels is provided in E.2.

NOTE 2 A method for selecting random generators is given in ISO/IEC 14888-3:2006, D.2.2.

— H: a hash-function that outputs a k-bit message digest.

The pair of keys of the signer is computed as follows.

a) The signer picks two integers, x_1 and x_2, uniformly at random from the range $[1, q - 1]$.

b) The signer computes $y = g_1^{-x_1} g_2^{-x_2}$.

The signature key is the pair (x_1, x_2) and the verification key is y.

6.2.3 Blind signature process

A blind signature process is an interactive protocol between a signer and a requestor. By executing the signing protocol, the requestor obtains a valid signature of a message of the requestor's choice in such a way that the signer learns nothing about the message or the resulting signature.

The signature process involves the following steps. The message to be blindly signed is denoted by m, where $m \in \{0, 1\}^*$.

a) The signer picks two integers, w_1 and w_2, uniformly at random from the range $[0, q - 1]$.

b) The signer computes $a = g_1^{w_1} g_2^{w_2}$.

c) The signer sends a to the requestor.

d) The requestor receives a from the signer.

e) The requestor picks an integer α uniformly at random from the range $[0, q - 1]$.

f) The requestor picks an integer β uniformly at random from the range $[0, q - 1]$.

g) The requestor picks an integer γ uniformly at random from the range $[0, q - 1]$.

h) The requestor computes $a' = a\, g_1^{\alpha} g_2^{\beta} y^{-\gamma}$.

i) The requestor computes $c' = H(m \,\|\, a')$.

j) The requestor computes $c = c' + \gamma \bmod q$.

k) The requestor sends c to the signer.

l) The signer receives c from the requestor.

m) The signer computes $r_1 = w_1 + c\,x_1 \bmod q$.

n) The signer computes $r_2 = w_2 + c\,x_2 \bmod q$.

o) The signer sends r_1 and r_2 to the requestor.

p) The requestor receives r_1 and r_2 from the signer.

q) The requestor checks that the values r_1 and r_2 have been correctly computed by verifying that $a = {g_1}^{r_1} {g_2}^{r_2} y^c$. If this verification fails, the requestor outputs reject and stops.

r) The requestor computes $r_1' = r_1 + \alpha \bmod q$.

s) The requestor computes $r_2' = r_2 + \beta \bmod q$.

t) The requestor sets the signature to $\sigma = (c', r_1', r_2')$.

6.2.4 Verification process

On input of a message, m, a signature $\sigma = (c', r_1', r_2')$, domain parameters, and the verification key, y, the verification process involves the following steps.

a) The verifier computes $a'' = {g_1}^{r_1'} {g_2}^{r_2'} y^{c'}$.

b) The verifier computes $c'' = H(m \,\|\, a'')$.

c) If $c'' = c'$ then return 1 (valid).

d) Else return 0 (invalid).

7 Blind signature mechanisms with partial disclosure

7.1 General

Clause 7 specifies two blind signature mechanisms with partial disclosure.

NOTE The mechanism in 7.2 is based on Reference [14], in which security proofs can also be found. The mechanism given in 7.3 is based on a scheme originally specified in Reference [17] and the associated security analysis is given in Reference [18].

7.2 Mechanism 2

7.2.1 Security parameters

The following symbol applies in the specification of this mechanism:

— l_q: a security parameter.

7.2.2 Key generation process

The key generation process of a blind signature mechanism consists of the following procedures:

a) generating domain parameters;

b) generating a private signature key and a public verification key.

The set of domain parameters includes the following parameters:

— q: a prime number satisfying $|q| = l_q$;

— G_q: a cyclic group of prime order q;

— g: a random generator of G_q;

— F: $\{0, 1\}^* \rightarrow G_q$ a cryptographic hash-function, where the discrete logarithm of value $F(x)$ in base g shall be unknown;

— H: $\{0, 1\}^* \rightarrow [0, q - 1]$ a hash-function.

NOTE 1 An example of recommended parameters for typical security levels is provided in E.2.

NOTE 2 Examples of how to construct F and H are provided in Annex D.

The pair of keys of the signer is computed as follows.

a) The signer picks an integer, x, uniformly at random from the range $[1, q - 1]$.

b) The signer computes $y = g^x$.

The signature key is x and the verification key is y.

7.2.3 Blind signature process with partial disclosure

The signature process involves the following steps. The message to be blindly signed is denoted by m, where $m \in \{0, 1\}^*$, and the common information is denoted by *info*, where *info* $\in \{0, 1\}^*$.

a) The signer picks three integers, u, s, d, uniformly at random from the range $[0, q - 1]$, and computes $z = F(info)$.

b) The signer computes $a = g^u$, $b = g^s z^d$.

c) The signer sends a, b to the requestor.

d) The requestor receives a, b from the signer.

e) The requestor picks two integers, t_1 and t_2, uniformly at random from the range $[0, q - 1]$.

f) The requestor picks two integers, t_3 and t_4, uniformly at random from the range $[0, q - 1]$.

g) The requestor computes $z = F(info)$.

h) The requestor computes $a' = ag^{t_1} y^{t_2}$, $b' = bg^{t_3} z^{t_4}$.

i) The requestor computes $e' = H(a' \| b' \| z \| m) \in [0, q - 1]$.

j) The requestor computes $e = e' - t_2 - t_4 \bmod q$.

k) The requestor sends e to the signer.

l) The signer receives e from the requestor.

m) The signer computes $c = e - d \bmod q$.

n) The signer computes $r = u - cx \bmod q$.

o) The signer sends r, c, s, d to the requestor.

p) The requestor receives r, c, s, d from the signer.

q) The requestor checks that the values r, c, s, d have been correctly computed by verifying that $a = g^r y^c$, $b = g^s z^d$, $e = c + d \bmod q$. If this verification fails, the requestor outputs reject and stops.

r) The requestor computes $r' = r + t_1$, $c' = c + t_2 \bmod q$.

s) The requestor computes $s' = s + t_3$, $d' = d + t_4 \bmod q$.

t) The requestor sets the signature to $\sigma = (r', c', s', d')$.

7.2.4 Verification process

On input of a message, m, a common information, $info$, a signature, $\sigma = (r', c', s', d')$, domain parameters, and the verification key, y, the verification process involves the following steps.

a) The verifier computes $z = F(info)$, $a' = g^{r'} y^{c'}$, $b' = g^{s'} z^{d'}$.

b) The verifier computes $e' = H(a' \| b' \| z \| m)$.

c) If $e' = c' + d' \bmod q$ then return 1 (valid).

d) Else return 0 (invalid).

7.3 Mechanism 3

7.3.1 Symbols

The following symbol applies in the specification of this mechanism:

— l_q: a security parameter.

7.3.2 Key generation process

The key generation process of a blind signature mechanism consists of the following procedures:

a) generating domain parameters;

b) generating a private signature key and a public verification key.

The set of domain parameters includes the following parameters:

— q: a prime number satisfying $|q| = l_q$;

— G_q: a cyclic group of prime order q;

— g_1: a random generator of G_q;

— g_2: a random generator of G_q different from g_1;

— H: $\{0, 1\}^* \rightarrow [0, q - 1]$ a cryptographic hash-function;

— H_1: $\{0, 1\}^* \rightarrow [0, q - 1]$ a cryptographic hash-function.

NOTE 1 An example of recommended parameters for typical security levels is provided in E.2.

NOTE 2 Examples of how to construct H and H_1 are provided in Annex D.

The pair of keys of the signer is computed as follows.

a) The signer picks an integer, x, uniformly at random from the range $[1, q - 1]$.

b) The signer computes $y_1 = g_1^x$.

c) The signer computes $y_2 = g_2^x$.

The signature key is x and the verification key is the pair (y_1, y_2).

7.3.3 Blind signature process with partial disclosure

The signature process involves the following steps. The message to be blindly signed is denoted by m, where $m \in \{0, 1\}^*$, and the common information is denoted by *info*, where *info* $\in \{0, 1\}^*$.

a) The signer picks an integer, ω, uniformly at random from the range $[0, q - 1]$.

b) The signer computes $g_M = {g_1}^{H_1(info)} g_2$.

c) The signer computes $t' = {g_M}^{\omega}$.

d) The signer sends t' to the signer.

e) The requestor receives t' from the signer.

f) The requestor picks two integers, λ and μ, uniformly at random from the range $[0, q - 1]$.

g) The requestor computes $g_M = {g_1}^{H_1(info)} g_2$.

h) The requestor computes $y_M = {y_1}^{H_1(info)} y_2$.

i) The requestor computes $t_M = t' {g_M}^{\lambda} {y_M}^{\mu}$.

j) The requestor computes $c = H(t_M \| info \| m)$.

k) The requestor computes $c' = c - \mu \bmod q$.

l) The requestor sends c' to the signer.

m) The signer receives c' from the requestor.

n) The signer computes $r' = \omega - c' x \bmod q$.

o) The signer sends r' to the requestor.

p) The requestor receives r' from the signer.

q) The requestor checks that the value r' has been correctly computed by verifying that $t' = {g_M}^{r'} {y_M}^{c'}$. If this verification fails, the requestor outputs reject and stops.

r) The requestor computes $r = r' + \lambda \bmod q$.

s) The requestor sets the signature to $\sigma = (c, r)$.

7.3.4 Verification process

On input of a message, m, a common information, *info*, a signature, $\sigma = (c, r)$, domain parameters, and the verification key, (y_1, y_2), the verification process involves the following steps.

a) The verifier computes $t'' = \left({g_1}^{H_1(info)} g_2\right)^r \left({y_1}^{H_1(info)} y_2\right)^c$.

b) The verifier computes $c'' = H(t'' \| info \| m)$.

c) If $c = c''$ then return 1 (valid).

d) Else return 0 (invalid).