DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 18370-2

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on:
2015-02-09

Voting terminates on:
2015-05-09

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

ICS: 35.040

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 18370-2:2014(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.

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.

ISO/IEC 18370-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *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 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 actual message 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 must conform to certain rules. They 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 of their 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. ISO/IEC 18370-2 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 and 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.

The mechanisms specified in this document 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.

DRAFT INTERNATIONAL STANDARD **ISO/IEC DIS 18370-2**

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 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 presentation process.

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

— the process for tracing requestors

— the process for tracing signatures

— the requestor tracing evidence evaluation process (optional); and,

— the signature tracing evidence evaluation process (optional).

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 18370-1, *Information technology — Security techniques — Blind digital signatures — Part 1: General*

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
cyclic group
group E of n elements that contains an element $a \in E$, called the generator, of order n.

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

3.2
finite commutative group
finite set E with the binary operation "$*$" such that

— for all $a, b, c \in E$, $(a * b) * c = a * (b * c)$

— there exists $e \in E$ with $e * a = a$ for all $a \in E$

— for all $a \in E$ there exists $b \in E$ with $b * a = e$

— for all $a, b \in E$, $a * b = b * a$

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 $a \in E$ is the least positive integer n such that $a^n = e$.

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

[SOURCE:ISO/IEC 14888-3:2006, 3.1]

3.3
pairing
function which takes two elements, P and Q, from an elliptic curve cyclic group over a finite field, G_1, as input, and produces an element from another cyclic group over a finite field, G_2, as output, and which has the following two properties (where we assume that the cyclic groups G_1 and G_2 have order q, for some prime q, and for any two elements P, Q, the output of the pairing function is written as $<P, Q>$)

— Bilinearity: if P, P_1, P_2, Q, Q_1, Q_2 are elements of G_1 and a is an integer satisfying $1 \leq a \leq q - 1$, then

$$< P_1 + P_2, Q> = < P_1, Q> * < P_2, Q>,$$

$$< P, Q_1 + Q_2> = < P, Q_1> * < P, Q_2>,$$

$$< [a]P, Q> = < P, [a]Q> = < P, Q>^a.$$

— Non-degeneracy: if P is a non-identity element of G_1, $<P, P> \neq 1$.

[SOURCE:ISO/IEC 14888-3:2006, 3.3]

3.4
security parameters
variables that determine the security strength of a mechanism

4 Symbols and abbreviated terms

For the purpose of this part of ISO/IEC 18370, the following symbols and abbreviations apply.

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

$a \| b$ concatenation of a and b in the order specified.

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

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

$|D|$ bit length of D if D is a bit string, or bit size of D if D is a 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 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, together with the point at infinity O_E

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

F_q The finite field consisting of exactly q 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 of the subgroup construction 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*.

H a cryptographic hash function

I a set of integers

$[n]P$ multiplication operation that takes a positive integer n and a point P on the curve E as input and produces as output another point Q on the curve E, where $Q = [n]P = P + P + \ldots + P$ 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 of size l_q-bit

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

$(a|p)$ The Legendre symbol of a and p where a is an integer and p is an odd prime number

$\prod_{(i \in I)} a_i$ 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 $x \leq y$.

<.,.> a bilinear and non-degenerate pairing

⟨…⟩ an ordered list of values to be hashed

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 prime field. Details of these two constructions are provided in Annex C.

5 General requirements

In order to use any of the mechanisms specified in this part of ISO/IEC 18370, the following requirements must 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; and,
- 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.

Before issuing a blind signature, the signer may 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 standard does not specify in which circumstances a requestor tracing process or a signature tracing process should be used.

6 Blind signature mechanisms

6.1 General

This clause specifies a blind signature mechanism.

NOTE The mechanism in this section is based on [19] and the associated security analysis is given in [22].

6.2 Mechanism 1

6.2.1 Security parameters

The following symbols apply in the specification of this mechanism.

- k, l_q: security parameters;

6.2.2 Key generation process

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

- generating domain parameters; and,
- 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. The outputs are a private signature key and the corresponding public verification key.

6.2.2.1 Generation of domain parameters

The set of domain parameters includes the following parameters:

— q a prime number of size l_q-bit;

— 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 An example of recommended parameters for typical security levels is provided in Annex E.2.

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

6.2.2.2 Generation of signature key and verification key

The signer computes a signature key as follows:

a) The signer randomly picks two integers x_1, x_2 from $[1, q\text{-}1]$

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 and 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 randomly picks two integers w_1, $w_2 \in [0, q - 1]$

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 chooses a random integer $\alpha \in [0, q - 1]$

f) The requestor chooses a random integer $\beta \in [0, q - 1]$

g) The requestor chooses a random integer $\gamma \in [0, q - 1]$

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 as $\sigma = (c', r_1', r_2')$

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

This clause specifies two blind signature mechanisms with partial disclosure.

NOTE The mechanism in 7.2 is based on [10] in which security proofs can also be found. The mechanism given in 7.3 is based on a scheme originally specified in [13] and the associated security analysis is given in [14].

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:

— generating domain parameters; and,

— generating a private signature key and a public verification key.

7.2.2.1 Generation of domain parameters

The set of domain parameters includes the following parameters:

— q a prime number of size l_q-bit;

— 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 should 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 Annex E.2.

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

7.2.2.2 Generation of signature key and verification key

A signer computes its signature key as follows:

a) The signer chooses a random integer $x \in [1, q\text{-}1]$

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 randomly picks three integers $u, s, d \in [0, q - 1]$, 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 chooses random integers $t_1, t_2 \in [0, q - 1]$

f) The requestor chooses random integers $t_3, t_4 \in [0, q - 1]$

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

h) The requestor computes $a' = ag^{t1}y^{t2}$, $b' = bg^{t3}z^{t4}$

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