INTERNATIONAL STANDARD

ISO/IEC 18370-1

First edition
2016-11-15

Information technology — Security techniques — Blind digital signatures —

Part 1: General

Technologie de l'information — Techniques de sécurité — Signatures numériques en blanc —

Partie 1: Généralités

Reference number
ISO/IEC 18370-1:2016(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

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 ISO documents 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 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 World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

A list of all parts in the ISO/IEC 18370 series can be found on the ISO website.

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and data integrity.

Blind signature mechanisms are a special type of digital signature mechanisms, as specified in ISO/IEC 9796 (all parts) and ISO/IEC 14888 (all parts), 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.

There are several variants of blind signature mechanisms. In some variants, the signer does not completely lose control over the signed message. In a blind signature mechanism with partial disclosure, the signer can include explicit information in the resulting signature based on an agreement with the requestor, whereas in a blind signature mechanism with selective disclosure, the choice of the message is restricted and conforms to certain rules. In other mechanisms, such as traceable blind signature mechanisms, an authorized entity is allowed to trace a signature to the requestor who requested it.

As is the case for conventional digital signature mechanisms, blind signature mechanisms are based on asymmetric cryptographic techniques and involve three basic operations:

- a process for generating a private signature key and a public verification key;
- a process for creating a blind signature that uses the private signature key;
- a process for verifying a blind signature that uses the public verification key.

Blind signatures and their variants can be used to provide users anonymity in a variety of electronic communication and transaction systems. Examples include Internet voting, electronic payment instruments, online auctions, public transport ticketing, road-toll pricing, and loyalty schemes. These mechanisms could also be used to achieve anonymous entity authentication. Anonymous entity authentication mechanisms are specified in ISO/IEC 20009 (all parts).

Like conventional digital signature mechanisms, the security of blind signature mechanisms 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 ISO/IEC 18370 (all parts) are based on the latter problem. However, security of some mechanisms also depends on the fact that some numbers are not only random but also unique.

The ISO/IEC 18370 series specifies three variants of blind signature mechanisms: blind signature mechanisms with partial disclosure, blind signature mechanisms with selective disclosure, and traceable blind signature mechanisms. This document specifies principles and requirements for these mechanisms. ISO/IEC 18370-2 specifies specific instances of these mechanisms.

The mechanisms specified in the ISO/IEC 18370 series use a variety of other standardized cryptographic algorithms, such as the following.

- They may use a collision-resistant hash-function to hash the message to be signed and to compute signatures. ISO/IEC 10118 (all parts) specifies hash-functions.
- They may use a conventional digital signature mechanism to certify public keys when such certification is required. Conventional digital signature mechanisms are specified in ISO/IEC 9796 (all parts) and ISO/IEC 14888 (all parts).
- They may require the use of a conventional entity authentication mechanism, if the signer needs to authenticate the requestor before issuing a blind signature. Entity authentication mechanisms are specified in ISO/IEC 9798 (all parts).
- They may require the use of a conventional asymmetric encryption mechanism, if certain information of the entities involved in the blind signature mechanism is required to be encrypted

for the purposes of privacy and confidentiality. Asymmetric encryption mechanisms are specified in ISO/IEC 18033-2.

Information technology — Security techniques — Blind digital signatures —

Part 1: General

1 Scope

This document specifies principles, including a general model, a set of entities, a number of processes, and general requirements for blind digital signature mechanisms, as well as the following variants of blind digital signature mechanisms:

- blind signature mechanisms with partial disclosure;
- blind signature mechanisms with selective disclosure;
- traceable blind signature mechanisms.

It also contains terms, definitions, abbreviated terms and figure elements that are used in all parts of ISO/IEC 18370.

See Annex A for a comparison on the blind digital signature mechanisms.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
attribute
application-specific *data element* (3.9)

3.2
blind signature
(digital) signature resulting from a *blind signature process* (3.3)

Note 1 to entry: The term “blind digital signature” may also be used because a blind signature is a special type of digital signature.

3.3
blind signature process
signature process (3.37) which allows a *requestor* (3.25) to obtain a *signature* (3.34) from a *signer* (3.45) over data of the requestor’s choice in such a way that both that data and the resulting signature are not made available to the *signer* (3.45)

3.4
blind signature process with partial disclosure
blind signature process (3.3) in which the *signer* (3.45) and the *requestor* (3.25) first agree on some information that will be attached to the *blind signature* (3.2)

Note 1 to entry: Such a process is sometimes referred to as a “partially blind signature process.”

3.5
blind signature process with selective disclosure
blind signature process (3.3) that allows a *requestor* (3.25) to receive a *blind signature* (3.2) on a *message* (3.17) not known to the *signer* (3.45) but which conforms to specific rules

3.6
blind signature with partial disclosure
signature (3.34) resulting from a *blind signature process with partial disclosure* (3.4)

Note 1 to entry: Such a signature is sometimes referred to as a “partially blind signature”.

3.7
blind signature with selective disclosure
signature (3.34) resulting from a *blind signature process with selective disclosure* (3.5)

3.8
collision-resistant hash-function
hash-function (3.14) satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

[SOURCE: ISO/IEC 10118-1:2016, 3.1]

3.9
data element
integer, bit string, set of integers, or set of bit strings

[SOURCE: ISO/IEC 14888-1:2008, 3.3]

3.10
distinguishing identifier
information which unambiguously distinguishes an entity

[SOURCE: ISO/IEC 11770-2:2008, 3.1]

3.11
domain
set of entities operating under a single security policy

3.12
domain parameter
data element (3.9) which is common to and known by or accessible to all entities within the *domain* (3.11)

[SOURCE: ISO/IEC 14888-1:2008, 3.5]

3.13
hash-code
string of bits which is the output of a *hash-function* (3.14)

[SOURCE: ISO/IEC 10118-1:2016, 3.3]

3.14
hash-function
function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, 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

[SOURCE: ISO/IEC 10118-1:2016, 3.4]

3.15
key
sequence of symbols that controls the operation of a cryptographic transformation

Note 1 to entry: Examples are encryption, decryption, cryptographic check function computation, signature generation, or signature verification.

[SOURCE: ISO/IEC 9798-1:2010, 3.16]

3.16
key pair
pair consisting of a *signature key* (3.36) and a *verification key* (3.51), i.e.,

— a set of *data elements* (3.9) that shall be totally or partially kept secret, to be used only by the *signer* (3.45);

— a set of *data elements* (3.9) that can be totally made public, to be used by any *verifier* (3.53)

[SOURCE: ISO/IEC 14888-1:2008, 3.9]

3.17
message
string of bits of any length

[SOURCE: ISO/IEC 14888-1:2008, 3.10]

3.18
parameter
integer, bit string, or *hash-function* (3.14)

[SOURCE: ISO/IEC 14888-1:2008, 3.11]

3.19
presentation process
process which takes as input the *message* (3.17) to be signed, the set of *message* (3.17) indices to disclose, the *token* (3.47), the token private *key* (3.15), and the signed array of disclosed *messages* (3.17) and gives as output a *presentation proof* (3.20)

3.20
presentation proof
signature on the *message* (3.17) to be signed using the token private *key* (3.15)

Note 1 to entry: This provides mathematical proof that the disclosed *messages* (3.17) were properly signed by the *signer* (3.45)

3.21
private requestor key
private *data element* (3.9) specific to a *requestor* (3.25) and usable only by this entity in a *traceable blind signature process* (3.49)

3.22
public requestor key
set of public *data elements* (3.9) which is mathematically related to a *private requestor key* (3.21)

3.23
public requestor tracing key
set of public *data elements* (3.9) which is mathematically related to a *requestor tracing key* (3.30)

3.24
public signature tracing key
set of public *data elements* (3.9) which is mathematically related to a *signature tracing key* (3.42)

3.25
requestor
entity which requests a *blind signature* (3.2) on a *message* (3.17) of the entity's choice from a *signer* (3.45) in a *signing session* (3.46)

3.26
requestor tracing authority
entity that can determine which *requestor* (3.25) requested the generation of a specified *blind signature* (3.2)

3.27
requestor tracing evidence
data element (3.9) which is an output of the *requestor tracing process* (3.31) and which substantiates the cryptographic binding between a *signature* (3.34) and the *distinguishing identifier* (3.10) of a *requestor* (3.25)

3.28
requestor tracing evidence evaluation process
process which takes as inputs a valid *blind signature* (3.2), *requestor tracing evidence* (3.27), the public *key* (3.15) of the *signer* (3.45), and *domain parameters* (3.12) and gives as output the result of *requestor tracing evidence* (3.27) evaluation: valid or invalid

Note 1 to entry: A valid *blind signature* (3.2) is a *blind signature* (3.2) that has been verified successfully using the *verification process* (3.52).

3.29
requestor tracing evidence evaluator
entity which checks the validity of *requestor tracing evidence* (3.27)

3.30
requestor tracing key
private *data element* (3.9) usable only by a *requestor tracing authority* (3.26) in the *requestor tracing process* (3.31)

3.31
requestor tracing process
process which gives as output the *distinguishing identifier* (3.10) of the *requestor* (3.25) which requested a given *signature* (3.34) and optionally also outputs *requestor tracing evidence* (3.27)

Note 1 to entry: This process is also called "re-identification" and sometimes referred to as "opening" in other standards, e.g. ISO/IEC 20009.

Note 2 to entry: Depending on the mechanism, the *requestor tracing process* (3.31) may output the *session identifier* (3.33) of the *blind signature* (3.2) request that resulted in this *signature* (3.34) instead of the requestor's *distinguishing identifier* (3.10).

3.32
security strength
number associated with the amount of work (that is the number of computational operations) that is required to break a cryptographic algorithm or system

Note 1 to entry: Security strength is specified in bits. A security strength of b bits means that of the order of 2^b operations are required to break the system. Common values of security strength are 80, 112, 128, 192, and 256.

3.33
session identifier
data element (3.9) used to unambiguously identify a *blind signature* (3.2) request, i.e. a *signing session* (3.46)

3.34
signature
one or more *data elements* (3.9) resulting from the *signature process* (3.37)

Note 1 to entry: A signature is also called a "digital signature."

[SOURCE: ISO/IEC 14888-1:2008, 3.12, modified — Note 1 to entry has been added.]

3.35
signature identifier
data element (3.9) resulting from the *signature tracing process* (3.43) which uniquely identifies the *signature* (3.34) yielded from a given *signing session* (3.46)

3.36
signature key
set of private *data elements* (3.9) specific to an entity and usable only by this entity in the *signature process* (3.37)

Note 1 to entry: A signature key is sometimes called a "private signature key" in other standards, e.g. ISO/IEC 9796-2 and ISO/IEC 9796-3.

3.37
signature process
process which takes as inputs data, the *signature key* (3.36), and the *domain parameters* (3.12), and which gives as output the data with a *signature* (3.34) over it

3.38
signature tracing authority
entity which can link a *signing session* (3.46) to the resulting *signature* (3.34)

3.39
signature tracing evidence
data element (3.9) which is an output of the *signature tracing process* (3.43) and which demonstrates the cryptographic binding between the *transcript of a signing session* (3.50) and a *signature identifier* (3.35)

3.40
signature tracing evidence evaluation process
process which takes as inputs the *transcript of a signing session* (3.50), a *signature identifier* (3.35), *signature tracing evidence* (3.39), the public key of the *signer* (3.45), and *domain parameters* (3.12) and gives as output the result of the evaluation of the *signature tracing evidence* (3.39): valid or invalid

3.41
signature tracing evidence evaluator
entity which checks the validity of *signature tracing evidence* (3.39)

3.42
signature tracing key
private *data element* (3.9) usable only by a *signature tracing authority* (3.38) in the *signature tracing process* (3.43)

3.43
signature tracing process
process which gives as output a *signature identifier* (3.35) which uniquely identifies the *signature* (3.34) yielded by a given *signing session* (3.46) and optionally also outputs evidence that the *signature identifier* (3.35) was correctly computed

3.44
signed message
set of *data elements* (3.9) consisting of the *signature* (3.34), the part of the *message* (3.17) which cannot be recovered from the *signature* (3.34), and an optional text field

[SOURCE: ISO/IEC 14888-1:2008, 3.15]

3.45
signer
entity generating a *blind signature* (3.2)

3.46
signing session
instance of a *blind signature process* (3.3)

Note 1 to entry: Although there are several exchanges in a session, a signing session is also sometimes called a “blind signature request.”

3.47
token
public *key* (3.15) and *signature* (3.34) resulting from a *blind signature process with selective disclosure* (3.5)

3.48
traceable blind signature
signature (3.34) resulting from a *traceable blind signature process* (3.49)

Note 1 to entry: Such a *signature* (3.34) is sometimes referred to as a “fair blind signature.”

3.49
traceable blind signature process
blind signature process (3.3) which allows a posteriori, a *requestor tracing authority* (3.26) (respectively a *signature tracing authority* (3.38)) to link a *signature* (3.34) to the *requestor* (3.25) which requested it (respectively to identify a *signature* (3.34) that resulted from a given *signature* (3.34) request)

Note 1 to entry: Such a process is sometimes referred to as a “fair blind signature process.”

3.50
transcript of a signing session
data elements (3.9) that the *signer* (3.45) can gather during a *signing session* (3.46)

Note 1 to entry: The transcript of a signing session is also called the “signer’s view.”

3.51
verification key
set of public *data elements* (3.9) which is mathematically related to an entity’s *signature key* (3.36) and which is used by the *verifier* (3.53) in the *verification process* (3.52)

Note 1 to entry: A verification key is sometimes called a “public verification key” in other standards, e.g. ISO/IEC 9796-2 and ISO/IEC 9796-3.