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

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 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.

3.52
verification process
process which takes as input the signed data, the digital signature, a valid *verification key* (3.51), and the *domain parameters* (3.12), and which gives as output the result of the signature verification: valid or invalid

[SOURCE: ISO/IEC 14888-1:2008, 3.17]

3.53
verifier
entity which checks the validity of a *blind signature* (3.2)

4 Abbreviated terms and figure elements

PK	public verification key
Rpk	public requestor key
Rsk	private requestor key
RTpk	public requestor tracing key
RTsk	requestor tracing key
SK	private signature key
STpk	public signature tracing key
STsk	signature tracing key

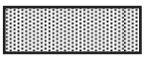

data


optional data


procedure


interactive procedure


entity in a procedure


data passed from one procedure to another


data flow


optional data flow

5 Blind signatures

5.1 General

A blind signature process is an interactive procedure conducted between a signer and a requestor. It allows a requestor to obtain a signature of a message of the requestor's choice without giving the signer any information about the actual message. Moreover, even if the signer sees, later on, one of the messages he or she signed, the signer will not be able to determine when and for whom he or she signed it.

A blind signature mechanism is defined by the specification of the following processes:

— a key generation process;

— a blind signature process;

— a verification process.

A blind signature mechanism shall satisfy the following security and privacy requirements.

— It is computationally infeasible, except for the signer, to produce more valid signatures than have been issued.

— It is computationally infeasible, even for the signer, to link a particular signature to a particular signing session.

Specific instances of blind signature mechanisms are specified in ISO/IEC 18370-2.

5.2 Entities

Three types of entities are involved in a blind signature mechanism, as listed below.

— Signer: a signer is an entity that generates a blind signature. This entity owns a key pair consisting of a signature key and a verification key.

— Requestor: a requestor is an entity that requests a blind signature from a signer in a signing session.

— Verifier: a verifier is an entity that verifies the validity of a blind signature.

5.3 Key generation

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

— generation of domain parameters;

— generation of 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 and the outputs are a private signature key and the corresponding public verification key.

Validation of domain parameters and keys may be required. However, any such procedure is outside the scope of the ISO/IEC 18370 series.

5.4 Blind signature process

A blind signature process, shown in Figure 1, is an interactive protocol conducted between a signer and a requestor. In this protocol, the signer takes as inputs the domain parameters, the verification key and the private signature key. The requestor takes as inputs the domain parameters, the verification key, and the message to be blindly signed.

If the protocol completes and does not abort, the output of the signer is a transcript of the signing session whereas the output of the requestor will be a signature on the message.

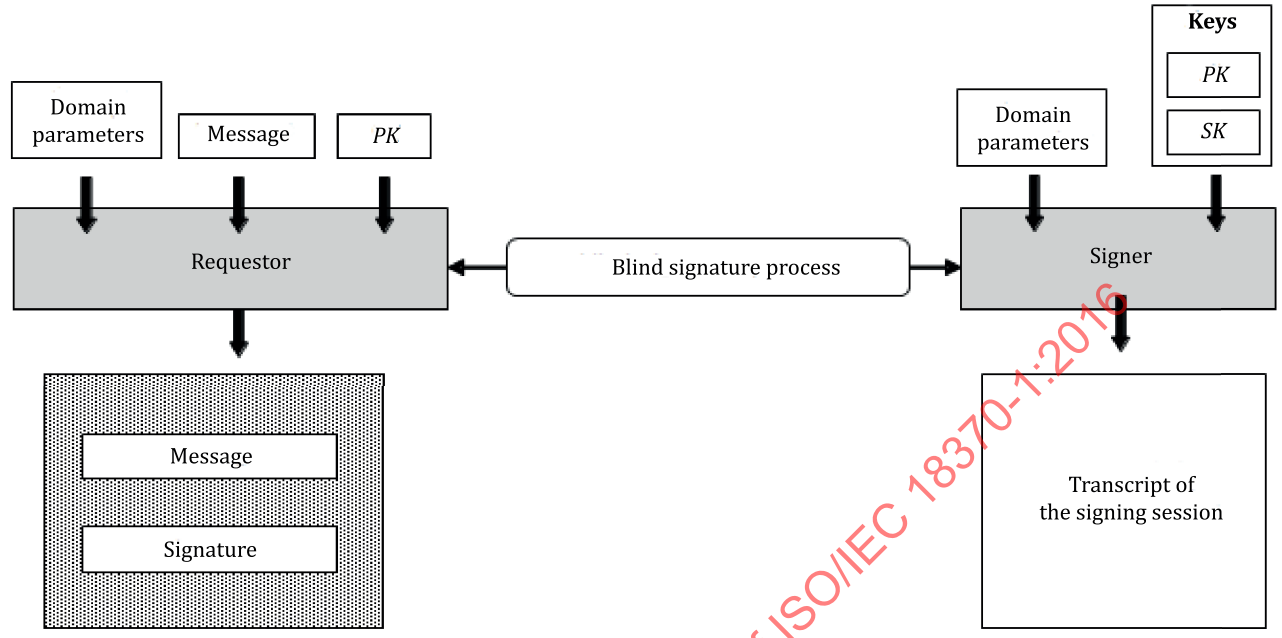


Figure 1 — Blind signature process

5.5 Verification process

The verification process, shown in Figure 2, is run by a verifier. It takes as input a signed message, the verification key, and the domain parameters, and gives as output the result of signature verification: valid or invalid.

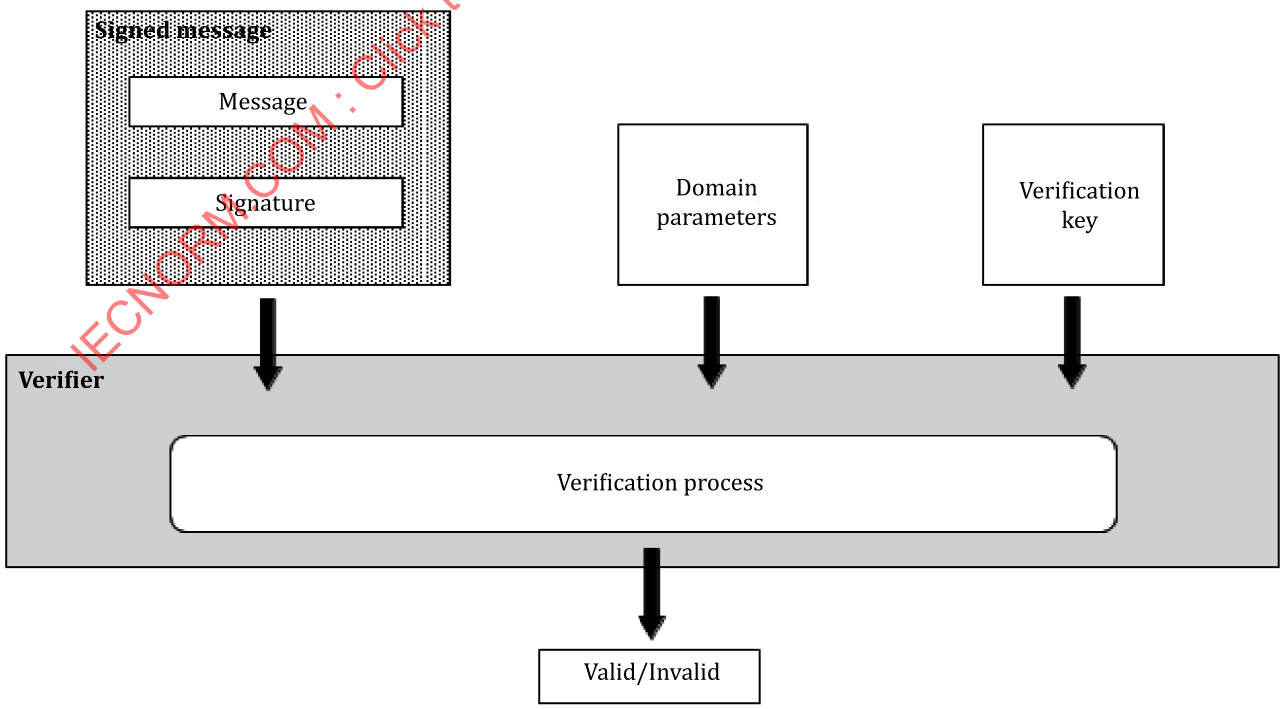


Figure 2 — Verification process

6 Blind signatures with partial disclosure

6.1 General

A blind signature mechanism with partial disclosure is a variant of a blind signature mechanism that allows a signer to explicitly include necessary information (e.g. an expiration date) in the resulting signature under an agreement with the requestor. Such a mechanism can be seen as a hybrid digital signature mechanism, which consists of a mix between a conventional (i.e. non-blind) digital signature mechanism and a blind signature mechanism.

A blind signature mechanism with partial disclosure is defined by the specification of the following processes:

— a key generation process;

— a blind signature process with partial disclosure;

— a verification process.

Specific instances of blind signature mechanisms with partial disclosure are specified in ISO/IEC 18370-2.

6.2 Entities

Three types of entities are involved in a blind signature mechanism with partial disclosure, as listed below.

— Signer: a signer is an entity that generates a blind signature with partial disclosure. This entity owns a key pair consisting of a signature key and a verification key.

— Requestor: a requestor is an entity that requests a blind signature with partial disclosure from a signer in a signing session.

— Verifier: a verifier is an entity that verifies the validity of a blind signature with partial disclosure.

6.3 Key generation

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

— generation of domain parameters;

— generation of 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.

NOTE Validation of domain parameters and keys can be required. However, any such procedure is outside the scope of the ISO/IEC 18370 series.

6.4 Blind signature process with partial disclosure

A blind signature process with partial disclosure, shown in Figure 3, is an interactive protocol conducted between a signer and a requestor. In this protocol, the message to be signed is divided in two parts: the first part, denoted as **info**, will be known by both entities, while the second part will be only known by the requestor.

The common information **info** may be supplied by either the signer or the requestor, or could be jointly determined by the signer and the requestor.

The negotiation of this common information, which should be performed prior to the execution of the blind signature process with partial disclosure, is outside the scope of the ISO/IEC 18370 series.

The inputs of the signer in this interactive protocol are the domain parameters, the common information **info,** the verification key, and the private signature key. The inputs of the requestor are the domain parameters, the verification key, the common information **info,** and the message to be blindly signed.

If the protocol completes and does not abort, the output of the signer is a transcript of the signing session. The output of the requestor will be a signature on the chosen message and on **info**.

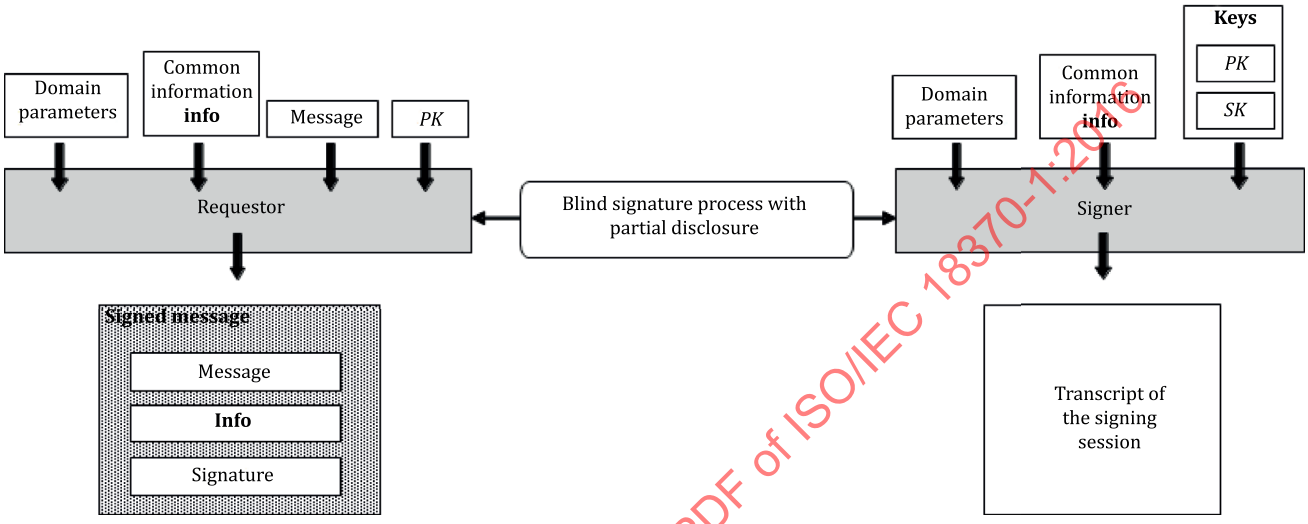


Figure 3 — Blind signature process with partial disclosure

6.5 Verification process

The verification process, shown in Figure 4, is run by a verifier. It takes as input a message, a signed message, the verification key, and the domain parameters. It gives as output the result of signature verification: valid or invalid.

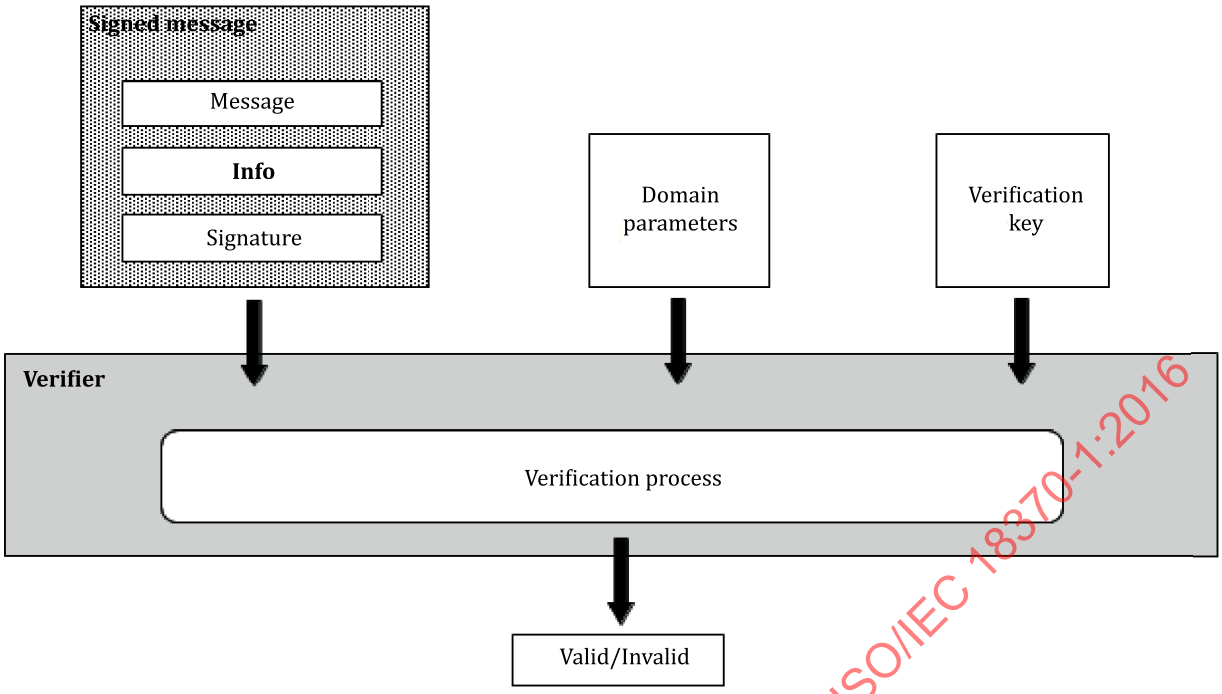


Figure 4 — Verification process

7 Blind signatures with selective disclosure

7.1 General

Blind signatures with selective disclosure are a type of a blind signature that allows a requestor to receive a blind signature on a message that is not known to the signer, and allows the requestor to selectively disclose information to other entities. The blind signature process with selective disclosure is an interactive protocol conducted between a signer and a requestor. By executing this protocol, the requestor obtains a valid signature on a vector of messages known to the signer, and a message and public key known only to the requestor, in such a way that the signer learns nothing about the resulting signature. The resulting public key and signature is called a "token." The token can be presented to a verifier using the corresponding private key as described in 7.5.

A blind signature mechanism with selective disclosure is defined by the specification of the following processes:

— a key generation process;

— a blind signature process with selective disclosure;

— a presentation process;

— a verification process.

A specific mechanism for blind signature with selective disclosure is specified in ISO/IEC 18370-2. See Annex B for additional information on the security information for blind signatures with selective disclosure.

7.2 Entities

Three types of entities are involved in a blind signature mechanism with selective disclosure, as listed below.

— Signer: a signer is an entity that generates a blind signature with selective disclosure. This entity owns a key pair consisting of a signature key and a verification key.

— Requestor: a requestor is an entity that requests a blind signature with selective disclosure from a signer, and generates a presentation proof for a verifier.

— Verifier: a verifier is an entity that verifies the validity of a blind signature with selective disclosure.

7.3 Key generation

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

— generation of domain parameters;

— generation of 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.

NOTE Validation of domain parameters and keys can be required to ensure that they were not generated in a way that could allow a party to contravene the security and privacy properties of this mechanism. However, any such procedure is outside the scope of the ISO/IEC 18370 series.

7.4 Blind signature process with selective disclosure

A blind signature process with selective disclosure, shown in Figure 5, is an interactive protocol conducted between a signer and a requestor. In this protocol, the signer takes as its inputs the domain parameters, the private signature key, the public verification key, and an array of messages to be signed.

The signer's signature is not a conventional digital signature [such as those produced using a mechanism defined in ISO/IEC 9796 (all parts) or ISO/IEC 14888 (all parts)], and because this is an interactive protocol, the requestor can hide selected parts of the array of messages from the signer when presenting them to a verifier. These messages can be used to encode application-specific data, such as signer-asserted attributes about the requestor.

The requestor takes as its inputs the domain parameters, the public verification key, and the array of messages to be signed. The output of this process is a token, which contains a public key and signature attesting to the validity of the messages and the public key, and a token private key.

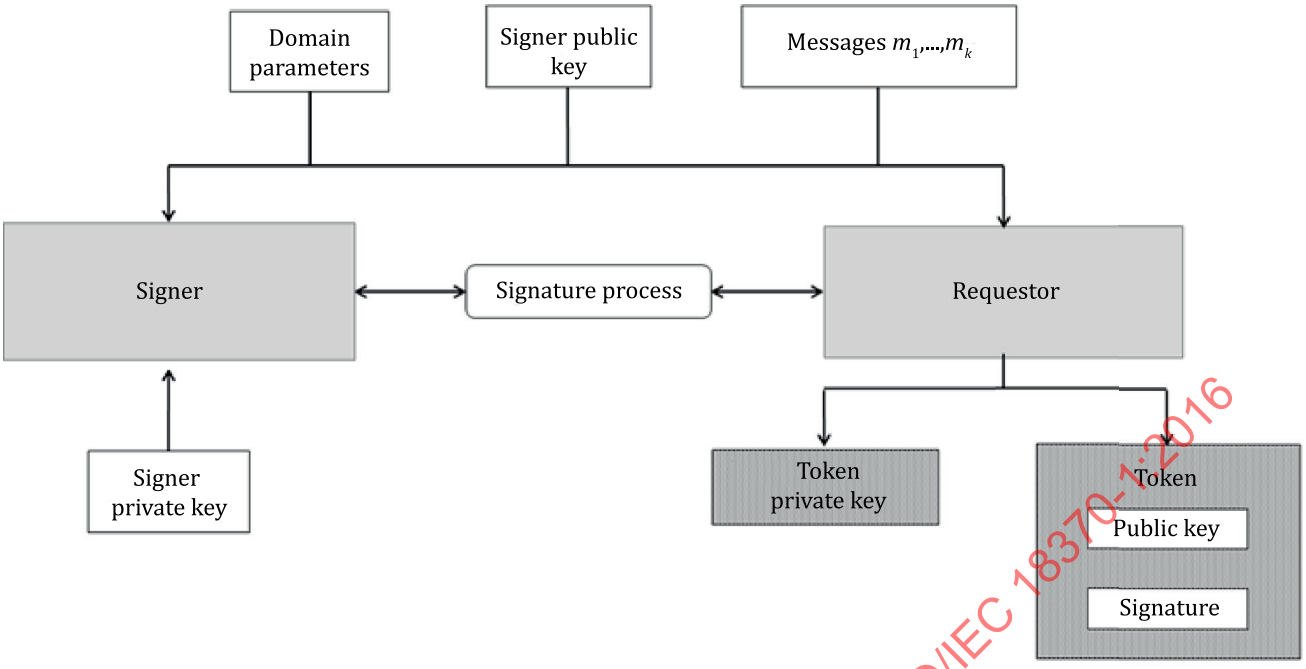


Figure 5 — Blind signature process with selective disclosure

7.5 Presentation process

A presentation process, shown in Figure 6, is performed by the requestor. The requestor takes as its inputs the domain parameters, the signer public key, the message to be signed by the requestor, the set of signer message indices to disclose, the token public key and signature, the token private key, and the array of messages signed by the signer. The output is a presentation proof, which contains a subset of the array of disclosed messages, and cryptographic material hiding the undisclosed messages.

NOTE The message signed by the requestor is different than the array of messages signed by the signer. The former allows the verifier to verify that the requestor used the private key corresponding to the token public key to sign the message (this can be used to encode a cryptographic challenge, or an application-specific statement); the latter allows the requestor to selectively present certified application-specific data from the signer to the verifier, without having the signer interacting with (or knowing about) the verifier.

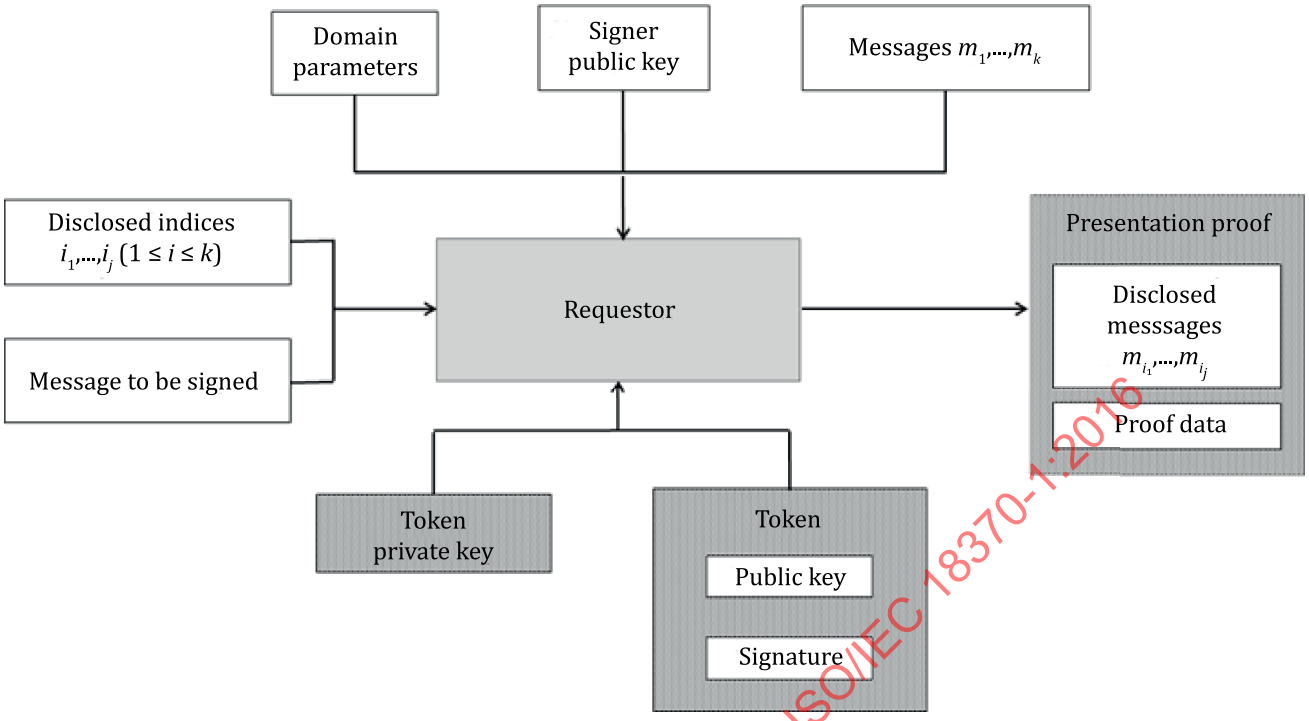


Figure 6 — Presentation process

7.6 Verification process

The verification process, shown in Figure 7, is performed by a verifier. The verifier takes as input domain parameters, the signer public key, the message signed by the requestor, the set of disclosed message indices, the token public key and signature, and the presentation proof. It gives as output the result of signature verification: valid or invalid.

Verification does not require any secret information or real-time communication with the signer or any other entity. All that is needed is an authentic copy of the domain parameters and signer public key under which the token was issued. A requestor can create arbitrarily many presentation proofs with the same token.

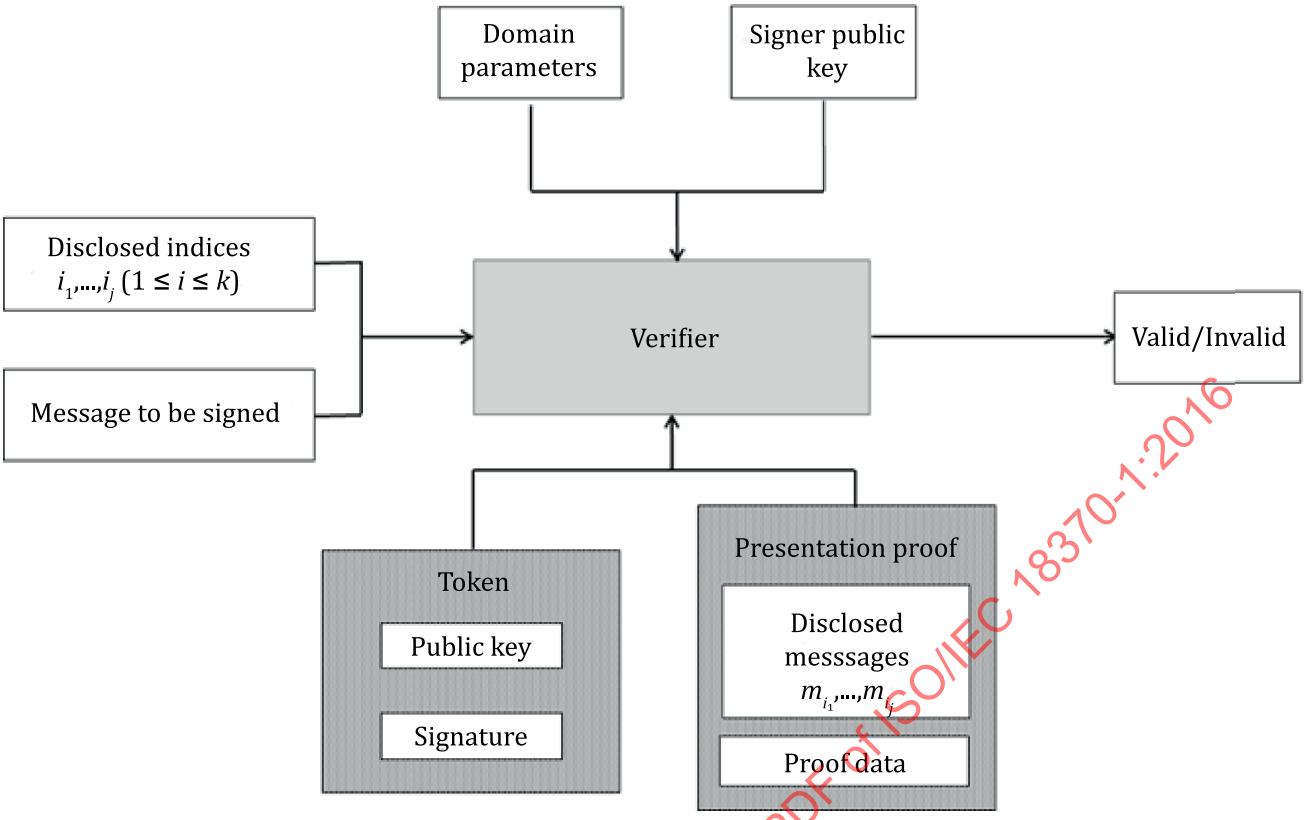


Figure 7 — Verification process

8 Traceable blind signatures

8.1 General

In a traceable blind signature mechanism, it may be possible to link a blind signature request to the resulting signature. Such a tracing mechanism can work in one of two ways: either it identifies a signature that resulted from a given signature request (signature tracing), or it links a signature to the requestor that requested it (requestor tracing). An entity that is capable of identifying a requestor from a signed message (or identifying a signature from a transcript of a signature request) is called a "requestor tracing authority" (or a "signature tracing authority," respectively).

A traceable blind signature mechanism is defined by the specification of the following processes:

— a key generation process;

— a traceable blind signature process;

— a verification process;

— a requestor tracing process;

— a signature tracing process;

— a requestor tracing evidence evaluation process (optional);

— a signature tracing evidence evaluation process (optional).

This document does not specify in which circumstances a requestor tracing process or a signature tracing process should be used.

Specific instances of traceable blind signature mechanisms are specified in ISO/IEC 18370-2.

8.2 Entities

Seven types of entities are involved in a traceable blind signature mechanism, as listed below.

— Signer: a signer is an entity that generates a traceable blind signature. This entity owns a key pair consisting of a signature key and a verification key.

— Requestor: a requestor is an entity that requests a traceable blind signature from a signer in a signing session. This entity owns a pair of keys consisting of a private requestor key and a public requestor key.

— Verifier: a verifier is an entity that verifies the validity of a traceable blind signature.

— Requestor tracing authority: a requestor tracing authority is an entity that identifies the requestor of a given traceable blind signature. Depending on the mechanism, the requestor tracing authority may output requestor tracing evidence, which indicates that a given signature is cryptographically bound to the distinguishing identifier of a requestor. Some mechanisms require that each requestor has a distinguishing identifier.

— Signature tracing authority: a signature tracing authority is an entity that links a signing session to the resulting signature. In some mechanisms, the requestor tracing authority and the signature tracing authority are the same entity.

— Requestor tracing evidence evaluator: a requestor tracing evidence evaluator is an entity that verifies the validity of requestor tracing evidence.

— Signature tracing evidence evaluator: a signature tracing evidence evaluator is an entity that verifies the validity of signature tracing evidence.

NOTE In some mechanisms, the distinguishing identifier of the requestor will correspond to the public requestor key.

8.3 Key generation

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

— generation of domain parameters;

— generation of a private signature key and a public verification key;

— generation of the requestor tracing key and the corresponding public requestor tracing key;

— generation of the signature tracing key and the corresponding public signature tracing key;

— generation of the private requestor key and the corresponding public requestor key.

The first procedure is executed once, when the domain is set up. The other procedures are executed for each signer, requestor, signature tracing authority, and requestor tracing authority within the domain.

NOTE Validation of domain parameters and keys can be required. However, any such procedure is outside the scope of the ISO/IEC 18370 series.

8.4 Traceable blind signature process

A traceable blind signature process, shown in Figure 8, is an interactive protocol conducted between a signer and a requestor. In this protocol, the signer takes as inputs the domain parameters, the public requestor key, the public requestor tracing key, the public signature tracing key, the verification key, and the private signature key. The requestor takes as inputs the domain parameters, the verification

key, the public requestor key, the public requestor tracing key, the public signature tracing key, the private requestor key, and the message to be blindly signed.

If the protocol completes and does not abort, the output of the signer is a transcript of the signing session whereas the output of the requestor will be the message along with a signature on this message.

The traceable blind signature process embeds the requestor's distinguishing identifier (respectively the signature identifier) in the signature (respectively in the transcript of the signing session) in such a way that the requestor tracing authority (respectively the signature tracing authority) can recover it but not any other party. This can be achieved by asymmetrically encrypting the distinguishing identifier (respectively the signature identifier) using the requestor tracing key (respectively the signature tracing key).

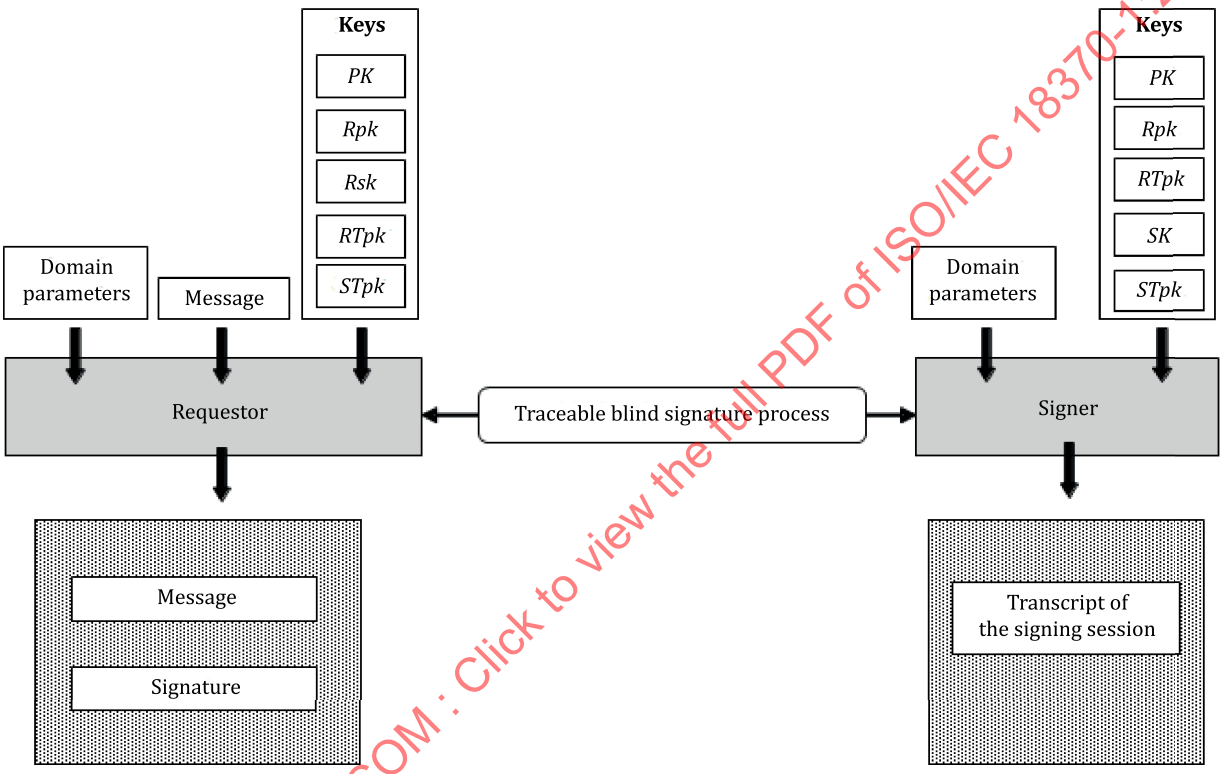


Figure 8 — Traceable blind signature process

8.5 Verification process

The verification process, shown in Figure 9, is run by a verifier. It takes as inputs a signed message, the verification key, the public requestor tracing key, the public signature tracing key and the domain parameters. It gives as output the result of signature verification: valid or invalid.

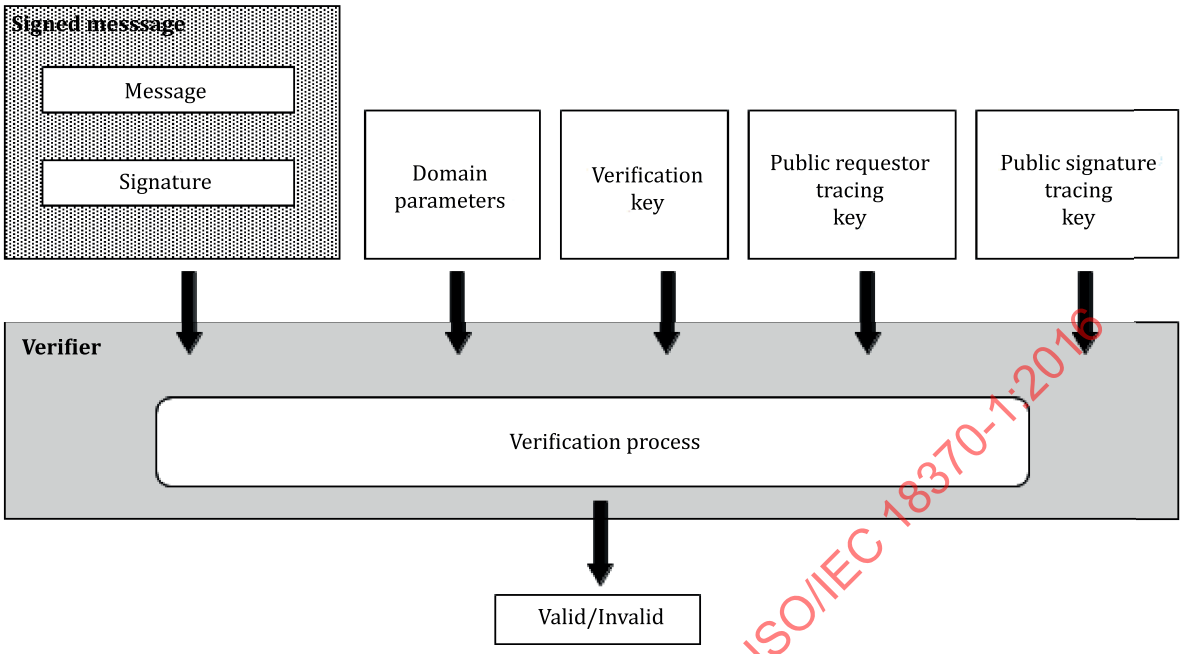


Figure 9 — Verification process

8.6 Requestor tracing process

The requestor tracing process, shown in Figure 10, is run by a requestor tracing authority. It takes as input a target traceable blind signature, the requestor tracing key, the public key of the signer, and domain parameters. It gives as output the distinguishing identifier of the requestor that requested this peculiar traceable blind signature.

Depending on the mechanism, the requestor tracing process may or may not involve a requestor tracing evidence evaluation process. If a requestor tracing evidence evaluation is required, the requestor tracing authority creates requestor tracing evidence, which demonstrates that the target signature is cryptographically bound to the output distinguishing identifier.

There are various reasons a requestor tracing process might or might not include a requestor tracing evaluation process. Generally, if the result of the requestor tracing process needs to be verified by an external evaluator, then the requestor tracing evidence evaluation process is used. The ISO/IEC 18370 series does not specify in which circumstances the requestor tracing evidence evaluation process should be used.

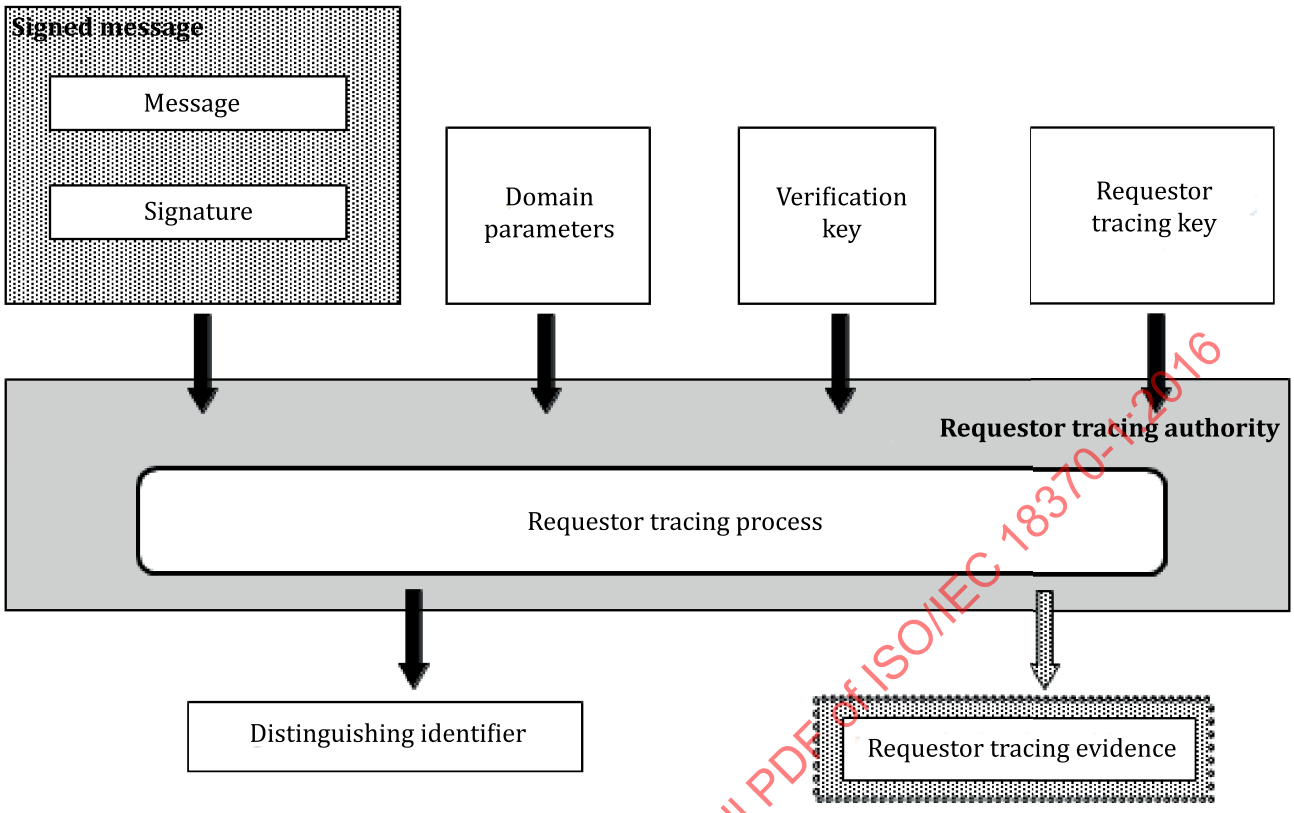


Figure 10 — Requestor tracing process

8.7 Requestor tracing evidence evaluation process

The requestor tracing evidence evaluation process, shown in Figure 11, is run by a requestor tracing evidence evaluator, which, based on requestor tracing evidence, checks whether or not a given traceable blind signature was requested by a specific requestor. If the requestor tracing evidence evaluator is convinced that the signature was requested by the requestor, the evaluator outputs valid; otherwise, it outputs invalid.

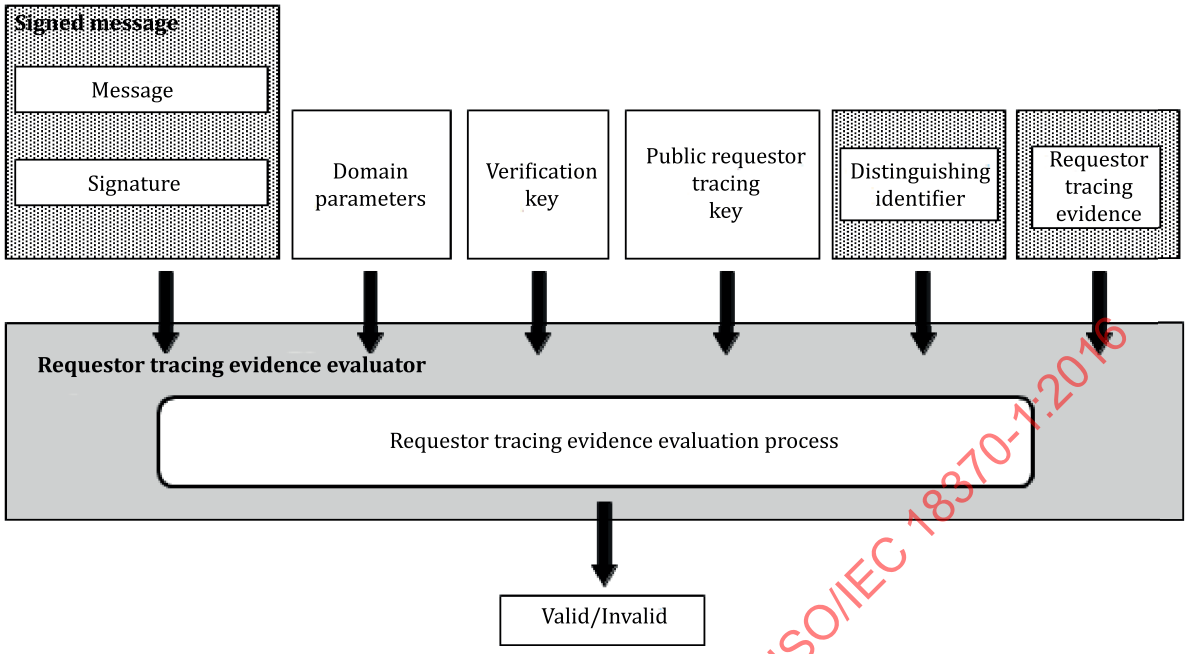


Figure 11 — Requestor tracing evidence evaluation process

8.8 Signature tracing process

The signature tracing process, shown in Figure 12, is performed by a signature tracing authority. It takes as inputs a target transcript of a signing session, the signature tracing key, the public key of the signer, and domain parameters. It gives as output a signature identifier that uniquely identifies the signature yielded from this signing session.

Depending on the mechanism, the signature tracing process may or may not involve a signature tracing evidence evaluation process. If a signature tracing evidence evaluation is required, the signature tracing authority creates signature tracing evidence that demonstrates the cryptographic binding between the given transcript of a signing session and the output signature identifier.

The ISO/IEC 18370 series does not specify in which circumstances the signature tracing evidence evaluation process should be used.