INTERNATIONAL STANDARD

ISO/IEC 20008-1

First edition
2013-12-15

Information technology — Security techniques — Anonymous digital signatures —

Part 1: General

Technologies de l'information — Techniques de sécurité — Signatures numériques anonymes —

Partie 1: Général

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

Reference number
ISO/IEC 20008-1:2013(E)

© ISO/IEC 2013

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

 © ISO/IEC 2013 – All rights reserved

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

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 20008-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 20008 consists of the following parts, under the general title *Information technology — Security techniques — Anonymous digital signatures*:

— *Part 1: General*

— *Part 2: Mechanisms using a group public key*

Further parts may follow.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

 © ISO/IEC 2013 – All rights reserved

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and data integrity. A digital signature mechanism enables the holder (or holders) of a private key (or keys) to singly or collectively generate a digital signature for a message. The corresponding verification key (or keys) can be used to verify the validity of the signature on the message. A digital signature mechanism satisfies the following requirements.

— Given either or both of the following:

  — the verification key but not the signature key,

  — a set of signatures on a sequence of messages that an attacker has adaptively chosen,

  it should be computationally infeasible for an attacker:

  — to produce a valid signature on a new message,

  — to recover the signature key, or

  — in some circumstances, to produce a different valid signature on a previously signed message.

— It should be computationally infeasible, even for the signer, to find two different messages with the same signature.

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

Anonymous digital signature mechanisms are a special type of digital signature mechanism. In an anonymous digital signature mechanism, given a digital signature, an unauthorised entity, including the verifier, cannot discover the signer's identifier. However, such a mechanism still has the property that only a legitimate signer can generate a valid signature. For authorised entities involved in an anonymous signature mechanism, there are four different cases:

a) a mechanism involving an authorised entity that is capable of identifying the signer of a signature;

b) a mechanism involving an authorised entity that is only capable of linking two signatures created by the same signer without identifying the signer;

c) a mechanism involving both of the authorised entities in Cases a) and b);

d) a mechanism involving neither of the authorised entities in Cases a) and b).

An example application of anonymous digital signatures is to achieve anonymous entity authentication. Anonymous entity authentication mechanisms are specified in ISO/IEC 20009.

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

— a process for generating private signature keys and public verification keys;

— a process for creating an anonymous digital signature that uses the signature key;

— a process for verifying an anonymous digital signature that uses the verification key.

NOTE A private signature key is also known as a signing key or a private key, and a public verification key is also known as a verification key or a public key.

One of the major differences between a conventional digital signature and an anonymous digital signature is in the nature of the public keys used to perform the signature verification. To verify a conventional digital signature, the verifier makes use of a single public verification key which is bound to the signer's identifier. To verify an anonymous digital signature, the verifier makes use of either a group public key or multiple public keys, which are not bound to an individual signer. In the literature,

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

an anonymous signature using a group public key is commonly known as a group signature, and an anonymous signature using multiple public keys is commonly known as a ring signature. The anonymity strength (i.e. degree of anonymity) provided by a mechanism depends upon the size of the group and the number of public keys.

Like conventional digital signature mechanisms, the security of anonymous digital signature mechanisms depends on 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 ISO/IEC 20008 are based on at least one of these and other similar problems.

ISO/IEC 20008 specifies anonymous digital signature mechanisms. This part of ISO/IEC 20008 specifies principles and requirements for two categories of anonymous digital signatures mechanisms: signature mechanisms using a group public key, and signature mechanisms using multiple public keys. ISO/IEC 20008-2 specifies a number of anonymous signature mechanisms in the first category.

NOTE If a business need for the development of mechanisms of the second category is discovered, then a new part of ISO/IEC 20008 should be added, which might, for example, be entitled Part 3: Mechanisms using multiple public keys.

The mechanisms specified in ISO/IEC 20008 use a variety of other standardised cryptographic algorithms, for example, as follows.

— They can use a collision resistant hash-function to hash the message to be signed and to compute signatures. ISO/IEC 10118 specifies hash-functions.

— They can 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 and ISO/IEC 14888.

— They can require the use of a conventional entity authentication mechanism, if the entities performing the mechanism require the data communicated as part of the mechanism to be authenticated. Entity authentication mechanisms are specified in ISO/IEC 9798.

— They can require the use of a conventional asymmetric encryption mechanism, if some information of the entities involved in the anonymous digital signature mechanisms is required to be encrypted for the purposes of privacy and confidentiality. Asymmetric encryption mechanisms are specified in ISO/IEC 18033-2.

Revocation is defined as 'the withdrawal of some power or authority that has been granted.' In the context of conventional digital signature mechanisms, it refers to withdrawing the power of a signing key that has been granted. Typically, a Certificate Revocation List is used for this purpose. Such a list specifies the certificate or public key corresponding to the signing key that needs to be revoked. A verifier can check whether or not a given signature was generated using a revoked signing key by checking the Certificate Revocation List. A verifier can also generate a personal blacklist of public keys as a local revocation list, and can then reject any signatures generated using a key corresponding to an entry in the list.

In an anonymous digital signature mechanism using multiple public keys, a public key can be revoked in the same way as in a conventional signature mechanism.

In an anonymous digital signature mechanism using a group public key, it is possible to revoke three different levels of authorization granted to an entity or a group of entities.

a) The entire group can be revoked.

b) The membership of a certain group member can be revoked. As a result, the revoked member is no longer authorised to create a group signature on behalf of the group.

c) A signature verifier can revoke the authorization for a group member to create a certain type of anonymous signature. After such a revocation, the member to whom the revocation applies might still be able to create other anonymous signatures on behalf of the group.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

 © ISO/IEC 2013 – All rights reserved

Information technology — Security techniques — Anonymous digital signatures —

Part 1: General

1 Scope

This part of ISO/IEC 20008 specifies principles, including a general model, a set of entities, a number of processes, and general requirements for the following two categories of anonymous digital signature mechanisms:

a) signature mechanisms using a group public key, and

b) signature mechanisms using multiple public keys.

2 Terms and definitions

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

2.1
anonymous digital signature
signature which can be verified using a group public key or multiple public keys, and which cannot be traced to the distinguishing identifier of its signer by any unauthorised entity including the signature verifier

Note 1 to entry: Anonymous digital signatures are also known as anonymous signatures or simply digital signatures.

2.2
anonymity strength
number derived from the probability that an unauthorised entity can correctly determine the true signer from a given signature

Note 1 to entry: An anonymity strength of n means that the probability that an unauthorised entity can correctly guess the true signer from a signature is $1/n$.

2.3
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

[SOURCE: ISO/IEC 10118-1:2000]

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment.

2.4
data element
integer, bit string, set of integers, or set of bit strings

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

2.5
distinguishing identifier
information which unambiguously distinguishes an entity

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

2.6
domain
set of entities operating under a single security policy

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

EXAMPLE Public key certificates created by a single authority or by a set of authorities using the same security policy.

2.7
domain parameter
data element which is common to and known by or accessible to all entities within the domain

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

2.8
evidence of binding
data element which demonstrates the cryptographic binding between the signer and the signature, and which is an output from the group membership opening process

2.9
evidence evaluation process
process which takes as inputs the evidence of binding, the group signature, and the group public key, and gives as output the result of evidence evaluation: valid or invalid

Note 1 to entry: The group signature input to an evidence evaluation process must be valid, i.e. the signature shall have previously been successfully verified using the group signature verification process.

2.10
evidence evaluator
entity which checks the validity of the evidence of binding

2.11
group
set of entities operating under a single membership management policy

Note 1 to entry: A group includes multiple group members and each member has a membership credential which is created by a group membership issuer as part of the group membership issuing process.

2.12
group member
entity which has a group membership credential and can create a group signature on behalf of the group

2.13
group member private key
private data element which is part of the group member signature key, specific to a group member and usable only by the member in the group membership issuing and group signature processes

2.14
group member signature key
set of data elements specific to a group member, consisting of the group member private key and group membership credential, and usable only by the member in the group signature process

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

2.15
group membership credential
data element specific to the group member, rendered unforgeable using the group membership issuing key, and usable by the group member in the group signature process

Note 1 to entry: The group membership credential is also called the membership credential.

Note 2 to entry: The group membership credential is part of the group member signature key.

2.16
group membership issuer
entity which creates group membership credentials

Note 1 to entry: The group membership issuer is also called the group issuer or the issuer.

2.17
group membership issuing key
private data element specific to a group membership issuer and usable only by the issuer in the group issuing process

Note 1 to entry: The group membership issuing key is also called the group issuing key or the issuing key.

2.18
group membership issuing process
process which takes as inputs the group membership issuing key, the group public key, the group public parameters, and optionally the distinguishing identifier, and which gives as output the group member signature key

Note 1 to entry: The group membership issuing process is also called the issuing process.

Note 2 to entry: The group membership issuing process is also referred to in the literature as the group member joining process or simply as the joining process.

2.19
global revocation
group signature revocation process which, by updating the group public key, other group public parameters, and/or revocation lists used in the group environment, has the effect of revoking the signature keys of some previously legitimate group members, who as a result become illegitimate

Note 1 to entry: A revocation list used in a global revocation process is also known as a group global revocation list.

Note 2 to entry: Group member signature keys might be updated in the global revocation.

2.20
group membership opener
entity which determines the identifier of the signer from a group signature

Note 1 to entry: The group membership opener is also called the group opener or the opener.

2.21
group membership opening key
private data element specific to a group membership opener and usable only by the opener in the group membership opening process

Note 1 to entry: The group membership opening key is also called the group opening key or the opening key.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

2.22
group membership opening process
process which takes as inputs the group signature, the group membership opening key, the group public key, and the group public parameters, and which gives as output the signer distinguishing identifier and optionally also gives evidence of binding between the signer and signature

Note 1 to entry: The group membership opening process is also called the opening process.

Note 2 to entry: It is required that the opening process takes as input a valid group signature, that means the signature has already been verified successfully using the group signature verification process.

2.23
group public key
public data element which is mathematically related to a group membership issuing key, and which is involved in the group membership issuing process, the group signature process, the group signature verification process, and optionally in any other processes of an anonymous signature mechanism using a group public key

Note 1 to entry: A group public key can be updated in some mechanisms for enabling revocation.

2.24
group public parameter
data element which is specific to the group and is accessible to all entities within the group, and which is involved in all the processes of an anonymous signature mechanism using a group public key

2.25
group signature
data element resulting from the group signature process

2.26
group signature linker
entity which determines whether or not two anonymous signatures are linked, i.e. they were created by the same signer

Note 1 to entry: The group signature linker is also called the linker.

Note 2 to entry: Depending on the mechanism, the linker might or might not possess a linking key.

2.27
group signature linking base
public data element, optionally specific to a group signature linker, which is involved in the group signature process if using this date element to link multiple signatures created by the same signer is required

Note 1 to entry: The group signature linking base is also called the linking base.

Note 2 to entry: The linking base is also sometimes referred to in the literature as the name base. This term is used in the specification of direct anonymous attestation given in ISO/IEC 20008-2.

2.28
group signature linking key
private data element specific to a group signature linker and usable only by the linker in the group signature linking process

Note 1 to entry: The group signature linking key is also called the linking key.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

2.29
group signature linking process
process which takes as inputs two anonymous signatures, the group public parameters, and optionally the group signature linking key, and which gives as output the result of the signature linkage: linked or not linked

Note 1 to entry: The group signature linking process is also called the linking process.

Note 2 to entry: In some ISO/IEC documents, e.g. ISO/IEC 20009-2, the linking process using a group signature linking key is referred to as providing local linking capability.

Note 3 to entry: Distinct signatures are linked if they were created under the same signature key and with the same parameters required for the linking process; distinct signatures are not linked if they were created under two different signature keys, or if they did not use the same parameters required for the linking process, for example, they were created under two different group signature linking bases.

2.30
group signature process
process which takes as inputs the message, the group member signature key, the group public key, the group public parameters, and optionally the linking base, and which gives as output the group signature

Note 1 to entry: The group signature process is also called the signature process.

2.31
group signature verification process
process which takes as inputs the group signed message, the group public key, and the group public parameters, and which gives as output the result of the group signature verification: valid or invalid

Note 1 to entry: The group signature verification process is also called the verification process.

2.32
group signature revocation list
data element which can be used to identify an anonymous signature that has been generated by a group member not authorised to create such a signature

Note 1 to entry: A group signature revocation list can include a range of types of content, including the private keys of revoked group members, components of revoked group membership credentials, and previously created signatures or partial signatures.

Note 2 to entry: Depending on the mechanism, a group signature revocation list can serve as a group public key revocation list, a group global revocation list, or a verifier local revocation list.

2.33
group signature revocation process
process which revokes the authorization of a group member to create a certain type of group signature

Note 1 to entry: A group signature revocation process can involve the revocation of an entire group, a group level global revocation, or a group signature verifier local revocation.

2.34
group signed message
signed message in which the signature is a group signature and which optionally includes a linking base

2.35
hash-code
string of bits which is the output of a hash-function

[SOURCE: ISO/IEC 10118-1:2000]

Note 1 to entry: The literature on this subject contains a variety of terms that have the same or similar meaning as hash-code. Modification Detection Code, Manipulation Detection Code, digest, hash-result, hash-value, and imprint are some examples.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

2.36
hash-function
function which maps strings of bits 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 10118-1:2000]

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment.

2.37
key
sequence of symbols that controls the operation of a cryptographic transformation

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

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

2.38
local revocation
group signature revocation process which enables a signature verifier to reject an invalid group signature on the basis of a group signature revocation list

Note 1 to entry: A group signature revocation list used in a local revocation process can be generated either by the verifier itself or by some other resource (e.g. it could be a part of a group global revocation list adopted by the verifier).

Note 2 to entry: A group signature revocation list used in a local revocation process is also known as a verifier local revocation list.

2.39
message
string of bits of any length

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

2.40
parameter
integer, bit string, or function

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

2.41
potential signer
entity whose public key is used by the true signer in the ring signature process

2.42
ring
set of entities consisting of the true signer and the potential signer (or signers)

2.43
ring public parameter
data element which is specific to the ring and is accessible to all entities involved in all the processes of anonymous signature mechanisms using multiple public keys

2.44
ring signature
data element resulting from the ring signature process

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

 © ISO/IEC 2013 – All rights reserved

2.45
ring signature process
process which takes as inputs the message, the signature key owned by the true signer, the public key (or keys) belonging to the potential signer (or signers), and the ring public parameters, and which gives as output the ring signature

2.46
ring signature verification process
process which takes as inputs the ring signed message, the public keys belonging to the true signer and potential signer (or signers), and the ring public parameters, and which gives as output the result of the ring signature verification: valid or invalid

2.47
ring signed message
signed message in which the signature is a ring signature

2.48
security strength
number associated with the amount of work (that is the number of 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.

2.49
signature
one or more data elements resulting from the signature process

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

2.50
signature key
set of private data elements specific to an entity and usable only by this entity in the signature process

Note 1 to entry: A signature key is sometimes called a private signature key, both in ISO/IEC 20008 and in other standards, e.g. ISO/IEC 9796-2 and ISO/IEC 9796-3.

2.51
signature key pair
pair of keys consisting of a signature key and a verification key, where:

— the signature key shall be kept partially or completely secret, and is intended for use only by the signer;

— the verification key can be made public, and is intended for use by any verifier

2.52
signature process
process which takes as inputs the message, the signature key, and the domain parameters, and which gives as output the signature

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

2.53
signed message
set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

2.54
signer
entity generating a digital signature

[SOURCE: ISO/IEC 13888-1:2009]

2.55
true signer
entity which creates a ring signature on behalf of the ring

Note 1 to entry: The true signer is also called the signer.

2.56
verification key
set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process

Note 1 to entry: A verification key is sometimes known as a public verification key, both in ISO/IEC 20008 and in other standards, e.g. ISO/IEC 9796-2 and ISO/IEC 9796-3.

2.57
verification process
process which takes as inputs the signed message, the verification key, and the domain parameters, and which gives as output the result of the signature verification: valid or invalid

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

2.58
verifier
entity which checks the validity of a signature

Note 1 to entry: The verifier is also known as the signature verifier.

3 Abbreviations and legend for figures

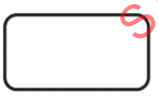
DAA Direct Anonymous Attestation

TPM Trusted Platform Module

The legend for the figures in this part of ISO/IEC 20008 is the following.


data


optional data


procedure


entity in procedure


data passed from one procedure to another

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

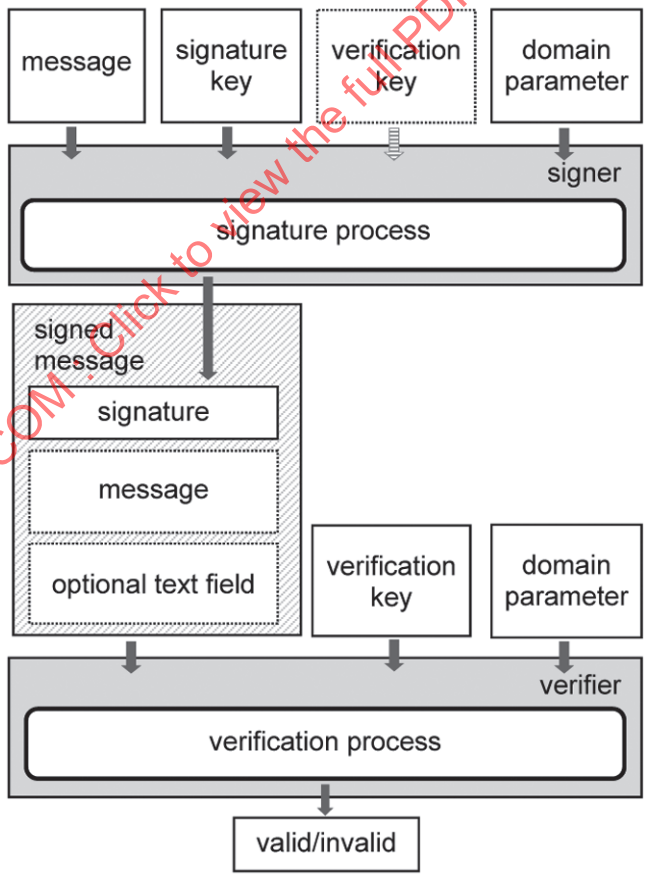
data flow

optional data flow

4 Options for a group public key and multiple public keys

In a conventional digital signature mechanism, as shown in Figure 1, a private signature key and a public verification key form a signature key pair. A signer uses the private signature key in the signature process to create a signature on a given message. A verifier uses the public verification key in the verification process to check whether or not the signature was signed under the corresponding private key. If the verifier is convinced that the signature was created using the signature key corresponding to the verification key, the verifier outputs *valid*; otherwise the verifier outputs *invalid*. As a result, from the verifier's point of view, the signature is bound to the signer via the public verification key, which acts as a distinguishing identifier for the signer.

In an anonymous digital signature mechanism, it is not necessary that a private signature key and a public verification key form a signature key pair, and that one is used in the signature process and the other is used in the verification process. This part of ISO/IEC 20008 specifies principles and requirements for two types of anonymous signature mechanisms which use different types of public verification keys. These two classes are known as mechanisms using a group public key and mechanisms using multiple public keys.



STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

Figure 1 — Signature & verification processes in a conventional signature mechanism

In an anonymous signature mechanism using a group public key, as shown in Figure 2, a signer is a group member. The group has a single group public key. Each group member has a distinct group member signature key which consists of the group member private key and a corresponding membership credential. A signer uses the group member signature key in the signature process to create a group

© ISO/IEC 2013 – All rights reserved

signature on a given message. A verifier uses the group public key in the group signature verification process to check whether or not the group signature was signed under a group member signature key, without revealing which of the group member signature keys was used to create the signature. If the verifier is convinced that the signature was created using one of the group member signature keys corresponding to the group public key, the verifier outputs *valid*; otherwise the verifier outputs *invalid*. As a result, from the verifier's point of view, the group signature is not bound to an individual signer, but is instead bound to the group via the group public key. The anonymity strength depends upon the size of the group.

NOTE Some mechanisms require a nonce generated by the verifier to be input to the group signature and group signature verification processes. For the purposes of Figure 2, the nonce is treated as part of the message.

In an anonymous signature mechanism using multiple public keys (also known as a ring signature mechanism), shown in Figure 3, each signer, including the true signer and each potential signer, has a private signature key and a public verification key which form a signature key pair in the same way as in a conventional digital signature mechanism. In the signature process, the true signer uses his signature key along with a public key (or a set of public keys), belonging to a potential signer (or a set of potential signers), to create a signature on a given message. In the verification process, a verifier uses a set of public keys containing those of the true signer and all the potential signers, to check whether or not the signature was signed under a signature key corresponding to a public key in the public key set without revealing which one. As a result, from the verifier's point of view, the signature is not bound to an individual signer, but is instead bound to the set of owners of the public keys. The anonymity strength depends upon the number of public keys.

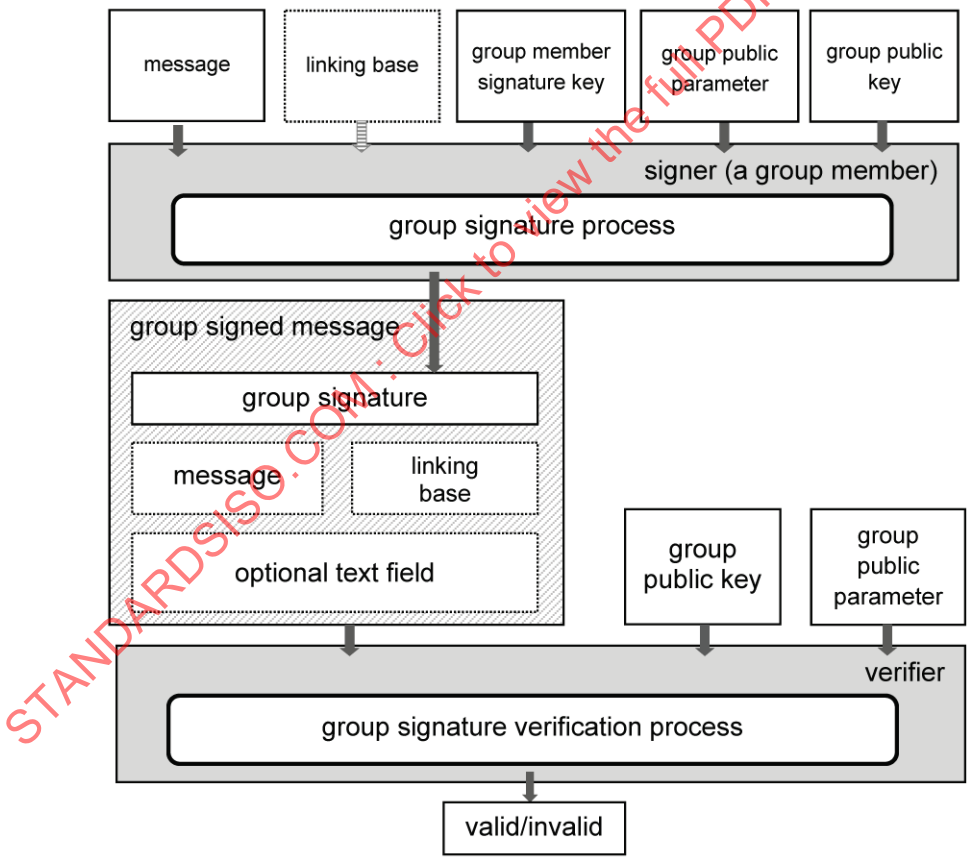


Figure 2 — Signature & verification processes in an anonymous signature mechanism using a group public key

As shown in Figures 1-3, the message input to the signature process may or may not be divided into two parts. If it is so divided, one part can be recovered from the signature and the other part cannot be

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

 © ISO/IEC 2013 – All rights reserved

recovered from the signature. The message part included in the signed message is the part which cannot be recovered from the signature.

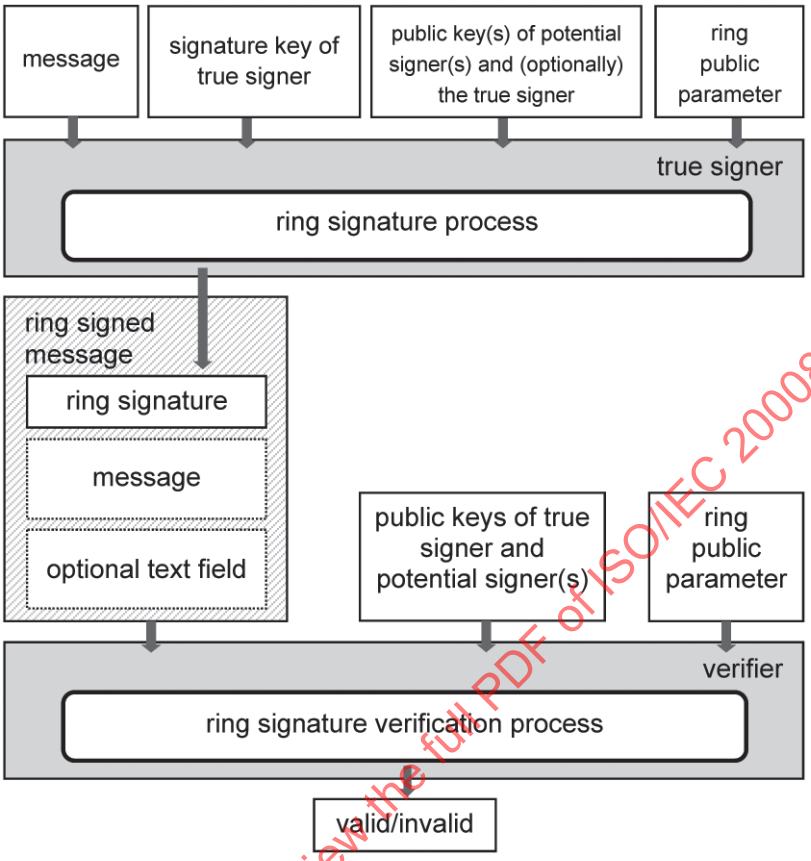


Figure 3 — Signature and verification processes for a ring signature mechanism

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

5 General requirements

Each entity involved in an anonymous digital signature mechanism shall be aware of a common set of domain parameters which are used to compute a variety of functions in the mechanism. In an anonymous signature mechanism using a group public key, the domain is associated with a group and the domain parameters are also known as group public parameters. In an anonymous signature mechanism using multiple public keys, the domain is associated with a ring and the domain parameters (also known as the ring public parameters) include all the parameters related to a set of public keys and the corresponding signature and verification processes.

Each signature verifier shall have access to an authentic copy of the necessary public keys. In an anonymous signature mechanism using a group public key, the public key belongs to a group of signers rather than an individual signer. In an anonymous signature mechanism using multiple public keys, the public keys are a set of individual public keys, each of which belongs to a true signer or a potential signer. The verifier is unable to distinguish a true signer from a potential signer.

Each signer shall have a distinguishing identifier which is unambiguously bound to the signer's private key. This information must be accessible to the relevant entities when performing the processes of the mechanism. In an anonymous signature mechanism using multiple public keys, the distinguishing identifier for a signer can be the signer's public verification key. In an anonymous signature mechanism using a group public key, the distinguishing identifier for a signer could take a variety of forms.

In an anonymous signature mechanism using a group public key, an entity authentication mechanism shall be used to allow a group member (as a signer) and a group membership issuer to run the group membership issuing process in an authentic manner. That ensures that the group membership issuer only

© ISO/IEC 2013 – All rights reserved

provides a group membership credential to a legitimate group member. When this entity authentication mechanism is not anonymous, use of one of the mechanisms specified in ISO/IEC 9798[3] is recommended. When this entity authentication mechanism is anonymous, use of one of the mechanisms specified in ISO/IEC 20009[13] is recommended.

ISO/IEC 20008 does not specify mechanisms for key management or for certification of group public keys or multiple individual public keys. A variety of means are available for obtaining a reliable copy of a public key, e.g., a public key certificate. Techniques for managing keys and certificates are outside the scope of ISO/IEC 20008. For further information, see ISO/IEC 9594-8,[1] ISO/IEC 11770-2,[5] ISO/IEC 11770-3[6] and ISO/IEC 15945.[10]

For anonymous signature mechanisms using a group public key, this standard does not specify how the group membership issuer authenticates a group member, and in which circumstances a group membership opening process or a group signature linking process is used. In addition it does not specify how a group membership issuer, a group membership opener, or any other entity decides that a group member is no longer authorised to create a certain type of group signature. However, when a revocation mechanism is used, it is required that each signature verifier has access to the latest group public key and any necessary group public parameters, and also that, if a group signature revocation list is in use, the verifier has access to it.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

6 Mechanisms using a group public key

6.1 General model

An anonymous digital signature mechanism using a group public key is also known as a group signature mechanism. This type of mechanism involves a group and a set of group members. There is a group membership issuer; also, if tracing a signature to its signer is required, a group membership opener is also required. The anonymity strength of the mechanism depends on the number of legitimate group members.

Depending on the mechanism, it may be possible to link two signatures created by the same signer. An entity which is capable of linking is known as a group signature linker; such an entity is not necessarily a member of the group. In some mechanisms, anyone can be a linker; in this case, a linking base is usually included in a signature. In other mechanisms, a linker must hold a group signature linking key; in this case, the public parameters corresponding to the linking key are included in a signature.

Depending on the mechanism, it may be possible to revoke a group member private key or a group membership credential; in either of these two cases a group member signature key will be revoked. A group signature created under a revoked group member signature key will be rejected during the group signature verification process.

An anonymous digital signature mechanism using a group public key is defined by the specification of the following processes:

— key generation process (including the group membership issuing process),

— group signature process,

— group signature verification process,

— group signature opening process (optional),

— group signature linking process (optional), and

— group signature revocation process (optional).

Specific instances of anonymous signature mechanisms using a group public key are specified in Part 2 of ISO/IEC 20008.

© ISO/IEC 2013 – All rights reserved

6.2 Entities

A number of types of entity are involved in an anonymous signature mechanism using a group public key, as listed below. Some types of entity are present in every mechanism, whereas others are only involved in mechanisms providing optional features.

— Signer: a signer is a group member that generates a digital signature. A signer owns a distinguishing identifier and a group member signature key, which consists of a group member private key and a membership credential.

NOTE 1 The group member signature key is sometimes known as the signer's signing key.

In some mechanisms, a signer role is split between multiple entities. For example, in Direct Anonymous Attestation (DAA) mechanisms, specified in Part 2 of ISO/IEC 20008, the signer role can be split between a principal signer with limited computational and storage capability, e.g. a Trusted Platform Module (TPM), and an assistant signer with more computational power but less security tolerance, e.g. an ordinary computer platform (namely the Host containing the embedded TPM).

NOTE 2 The TPM technology is specified in ISO/IEC 11889[7].

— Verifier: a verifier is an entity verifying a digital signature.

— Group membership issuer: a group membership issuer is an entity issuing a group membership credential to a signer. This entity exists in all the mechanisms specified in Part 2 of ISO/IEC 20008.

— Group membership opener: a group membership opener is an entity that determines the signer of a signature. This entity exists in some of the mechanisms specified in Part 2 of ISO/IEC 20008. In some mechanisms, the group membership issuer and the group membership opener are the same entity. Depending on the mechanism, the group membership opener may output evidence of binding, that binds the signature to its signer's distinguishing identity.

— Evidence evaluator: an evidence evaluator checks the validity of the evidence of binding.

— Group signature linker: a group signature linker is an entity that is capable of linking two signatures generated by the same signer. This entity exists in some of the mechanisms specified in Part 2 of ISO/IEC 20008. In some mechanisms, the linker is also the verifier. The number of linkers in an anonymous signature mechanism may vary.

6.3 Key generation process

The key generation process includes key generation algorithms for creating the group membership issuing key, the group membership opening key, and the group signature linking key (or keys) if they are required in the mechanism. A typical key generation algorithm takes as input a security parameter which is dependent on the security strength of the mechanism, and gives as output a private and public key pair.

The key generation process also includes a group membership issuing process. Depending on the mechanism, the group membership issuing process, as shown in Figure 4, may or may not involve a protocol between a user who wishes to become a group member and a group membership issuer.

If such a protocol is required, both the group member and group membership issuer shall contribute to generation of the group member signature key. On completion of the protocol, the group member possesses a group member signature key, which consists of the member's group member private key and membership credential; the group membership issuer will know the membership credential and the distinguishing identifier of the member, which are related to each other. The form of the distinguishing identifier depends on the mechanism, and it may or may not be input to the group membership issuing process.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

Alternatively, the group membership issuer shall solely generate the group member signature key, and give it to the group member. In this case, a group member private key and membership credential are not distinct, and both the member and issuer shall be in possession of the value of the signature key.

NOTE If the group membership issuer knows the signer's group member signature key, the group membership issuer must be trusted not to impersonate a group member. Otherwise the group signature mechanism will not possess the non-repudiation property.

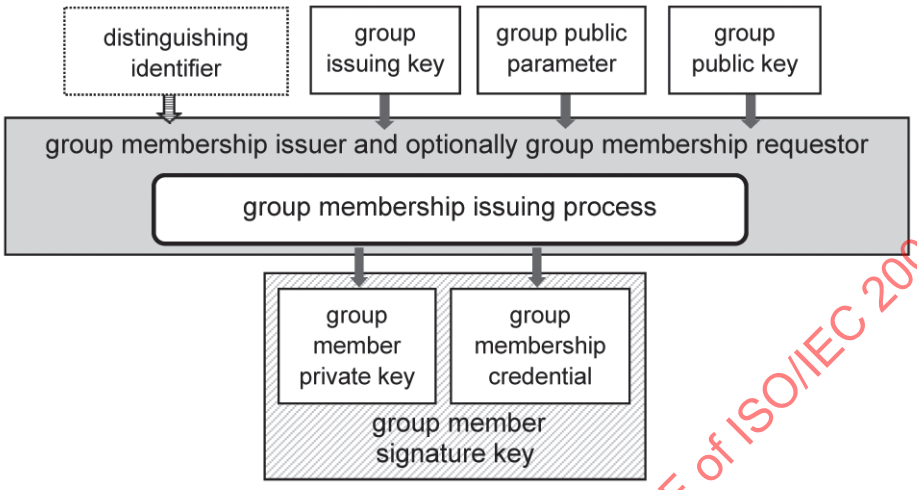


Figure 4 — Group membership issuing process

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

6.4 Group signature process

The signature process is performed by a group member acting as a signer. The signer uses its member signature key to compute a group signature on a given message.

If the mechanism supports group membership opening, the signature process will embed the distinguishing identifier in the signature in such a way that the group membership opener can recover it but not any other party. This can be achieved by asymmetrically encrypting the distinguishing identifier using the group opener's public key before inclusion in the signature.

If the mechanism supports group signature linking, the signature process will use the same linking base or linking key when generating two signatures that are to be linkable, in such a way that the group signature linker can link them but not any other party. Depending on the mechanism, the linker may or may not be a signature verifier.

If the mechanism allows signers to be revoked, the signature process shall include functionality that ensures a verifier can verify that a signature was created by a non-revoked signer.

6.5 Group signature verification process

The verification process is performed by a verifier, who is able to associate the correct group public key with the signature, but is not able to determine the identifier of the signer from the signature.

Depending on the mechanism, the verification process may or may not be independent of a signature linking process and/or a signature revocation process.

6.6 Group membership opening process

The opening process, shown in Figure 5, is performed by a group membership opener. It enables the opener to determine the distinguishing identifier of the signer of an anonymous signature.

 © ISO/IEC 2013 – All rights reserved

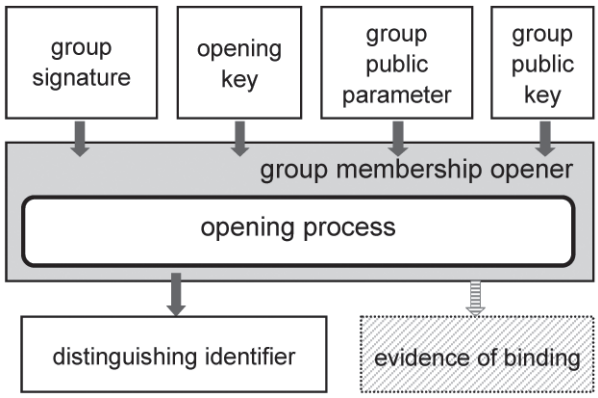


Figure 5 — Group membership opening process

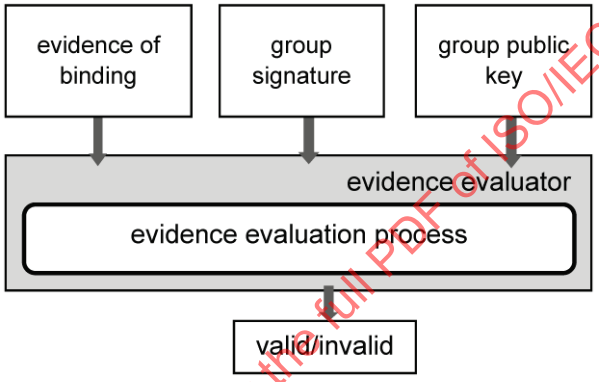


Figure 6 — Evidence evaluation process

Depending on the mechanism, it may or may not involve an evidence evaluation process. If evidence evaluation is required, in the opening process the group membership opener creates evidence of binding, which indicates that a given signature is cryptographically bound to the distinguishing identifier of the signer. The evidence evaluation process, as shown in Figure 6, is performed by an evidence evaluator, which, based on the evidence of binding, checks whether or not the opener has correctly identified the signer from a given signature. If the evidence evaluator is convinced that the signature matches with the evidence of binding, the evaluator outputs *valid*; otherwise, the evaluator outputs *invalid*.

NOTE There are various reasons why an opening process might or might not include an evidence evaluation process. Generally speaking if the result of the opening process needs to be verified by an external evaluator, then the evidence evaluation process is used. How to decide whether or not to include the evidence evaluation process as part of the opening process is outside the scope of this part of ISO/IEC 20008.

6.7 Group signature linking process

The group signature linking process, shown in Figure 7, is performed by a group signature linker, who checks whether or not two given valid signatures were created by the same signer. Depending on the mechanism, the group signature linker may or may not have a linking key. Also depending on the mechanism, the group signature linking process may or may not involve a linking base, which may or may not be created by the group signature linker. If such a linking base is required, it is used in the group signature process when creating both the signatures.

NOTE A mechanism incorporating a linking process is said to possess the property of user-controlled-linkability or controllable linkability (e.g. [14]).

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

© ISO/IEC 2013 – All rights reserved

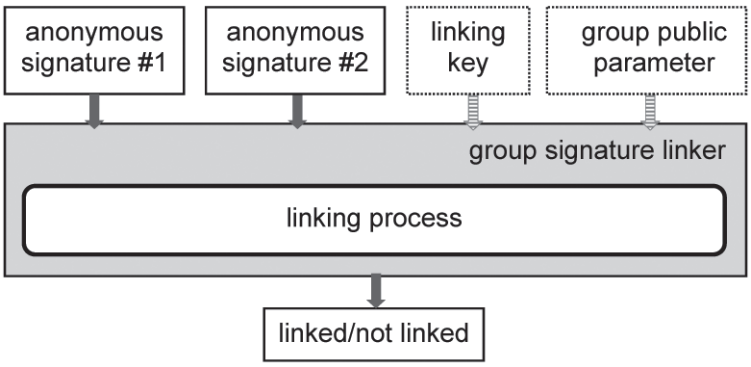


Figure 7 — Group signature linking process

6.8 Group signature revocation process

6.8.1 General

Three different 'levels' of revocation can be defined for an anonymous digital signature mechanism using a group public key. These three levels allow different types of authorizations to be revoked.

6.8.2 Level 1 revocation

The entire group is revoked. If the authorization of an entire group needs to be revoked, the appropriate group public key shall be added to a group public key revocation list. Any anonymous digital signatures associated with a revoked group public key shall be rejected. This revocation method is the same as that used with a conventional digital signature scheme.

NOTE Mechanisms for this type of revocation are not specified in ISO/IEC 20008-2.

6.8.3 Level 2 revocation

The membership of a specified group member is revoked, and as a result the revoked member is no longer authorised to create group signatures on behalf of the group. This shall be achieved using one of the following two methods.

a) A group membership issuer updates the group public key (which might or might not involve updating its private key and/or the group public parameters). The issuer then updates the credentials of all legitimate signers using the new group public key. In subsequent uses of the group signature process, verification process, opening process and linking process, the newly updated keys and credentials will be used. Depending on the mechanism, this updating method may be performed regularly, whenever the group membership issuer wishes to revoke certain group members, or in both cases.

   NOTE 1 This revocation method is known as rekey-based revocation or credential update revocation.

   NOTE 2 Depending on the mechanism, one of two different procedures can be involved in this revocation method. In the first, a group issuer interacts with each legitimate group member to update the member's group membership signature key. In the second, a group Issuer creates certain public information and then each legitimate group member updates its own group membership signature key accordingly to this information.

b) An alternative method makes use of a group global revocation list. The contents of such a revocation list depend on the mechanism, and a number of general cases are specified below. An anonymous digital signature associated with an authorization specified in the group global revocation list shall be rejected by a group signature verifier.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 20008-1:2013

 © ISO/IEC 2013 – All rights reserved