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

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

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

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.

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.

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,

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.

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]

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

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.

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.

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.