INTERNATIONAL STANDARD

ISO/IEC 20008-2

First edition
2013-11-15

Information technology — Security techniques — Anonymous digital signatures —

Part 2: Mechanisms using a group public key

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

Partie 2: Mécanismes utilisant une clé publique de groupe

Reference number
ISO/IEC 20008-2:2013(E)

COPYRIGHT PROTECTED DOCUMENT

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.

ISO/IEC 20008-2 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

Anonymous digital signature mechanisms are a special type of digital signature mechanism in which, given a digital signature, an unauthorized entity cannot discover the signer's identifier yet can verify that a legitimate signer has generated a valid signature.

ISO/IEC 20008 specifies anonymous digital signature mechanisms. ISO/IEC 20008-1 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. This part of ISO/IEC 20008 specifies a number of anonymous signature mechanisms of the first category.

Anonymous signature mechanisms of the first category can have capabilities for providing more information about the signer. Some have a linking capability, where two signatures signed by the same signer are linkable. Some have an opening capability, where the signature can be opened by a special entity to reveal the identity of the signer. Some have both linking and opening capabilities.

For each mechanism, the processes of opening, linking, and/or revocation are specified.

The mechanisms specified in this part of ISO/IEC 20008 use a collision-resistant hash-function. A hash-function specified in ISO/IEC 10118 is to be used.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity, and scope of these patent rights.

The holders of these patent right have assured the ISO and IEC that they are willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from:

— Electronics and Telecommunications Research Institute (ETRI)

  161, Gajeong-dong, Yuseong-gu, Daejeon, Korea

— NEC Corporation

  7-1, Shiba 5-chome, Minato-Ku, Toyko 108-8001, Japan

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and/or IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

Information technology — Security techniques — Anonymous digital signatures —

Part 2: Mechanisms using a group public key

1 Scope

This part of ISO/IEC 20008 specifies anonymous digital signature mechanisms, in which a verifier makes use of a group public key to verify a digital signature.

It provides

— a general description of an anonymous digital signature mechanism using a group public key, and

— a variety of mechanisms that provide such anonymous digital signatures.

For each mechanism, this part of ISO/IEC 20008 specifies

— the process for generating group member signature keys and a group public key,

— the process for producing signatures,

— the process for verifying signatures,

— the process for opening signatures (if the mechanism supports opening),

— the process for linking signatures (if the mechanism supports linking), and

— the process for revoking group members.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

ISO/IEC 15946-5, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

ISO/IEC 18032, *Information technology — Security techniques — Prime number generation*

ISO/IEC 20008-1, *Information technology — Security techniques — Anonymous digital signatures — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20008-1 and the following apply.

3.1
assistant signer
entity that can help a principal signer to create anonymous signatures, but that cannot generate anonymous signatures unaided

3.2
member-list
list that includes the identities of group members together with their corresponding group membership credentials

3.3
principal signer
entity which is in possession of a group member signature key and which can create anonymous signatures using this key

3.4
secret seed value
secret data known to a group member and used for deriving group member private keys

3.5
security parameters
variables that determine the security strength of a mechanism

4 Symbols (and abbreviated terms)

For the purposes of this part of ISO/IEC 20008, the following symbols and abbreviations apply.

bsn	Linking base, either a special symbol $\perp$ or an arbitrary string.
e	A bilinear map function $e: G_1 \times G_2 \rightarrow G_T$ such that for all $P \in G_1$, $Q \in G_2$, and all positive integers a, b, the equation $e([a]P, [b]Q) = e(P, Q)^{ab}$ holds. This function is also called a pairing function.
gcd(a, b)	The greatest common divisor of the integers a and b.
G_1	An additive cyclic group of order p over an elliptic curve.
G_2	An additive cyclic group of order p over an elliptic curve.
G_T	A multiplicative cyclic group of order p.
H	A cryptographic hash-function.
m	Message to be signed.
n	An RSA modulus where $n = pq$.
O_E	The elliptic curve point at infinity.
p	A prime number.
P_1	Generator of G_1.
P_2	Generator of G_2.
q	A prime number.
Q_1+Q_2	The elliptic curve sum of points Q_1 and Q_2.
QR(n)	The group of quadratic residues modulo n.

Z_n^* The multiplicative group of invertible elements in Z_n.

Z_p The set of integers in [0, p-1].

Z_p^* The set of integers in [1, p-1].

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

$[n]P$ Multiplication operation that takes a positive integer n and a point P on the elliptic curve E as input and produces as output another point Q on the curve E, where $Q = [n]P = P + P + \ldots + P$, i.e., the sum of n copies of P. The operation satisfies $[0]P = O_E$ and $[-n]P = [n](-P)$.

$[x, y]$ The set of integers from x to y inclusive, if x, y are integers satisfying $x \le y$.

|| $X \| Y$ is used to mean the result of the concatenation of data items X and Y in the order specified. In cases where the result of concatenating two or more data items is signed as part of one of the mechanisms specified in this part of ISO/IEC 20008, this result shall be composed so that it can be uniquely resolved into its constituent data strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property could be achieved in a variety of different ways, depending on the application. For example, it could be guaranteed by (a) fixing the length of each of the substrings throughout the domain of use of the mechanism, or (b) encoding the sequence of concatenated strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1.[1]

5 General model and requirements

This clause specifies the general model and requirements for the anonymous digital signature mechanisms specified in this part of ISO/IEC 20008. Some of the contents of this clause are taken from Part 1 of this international standard. In addition, specific requirements applying to mechanisms using a group public key are addressed.

An anonymous digital signature mechanism using a group public key involves a group and a set of group members. Each group shall possess a group membership issuer. There may also be a group membership opener and/or a group signature linker, depending on the mechanism. Multiple entities may function in the role of a group membership opener or a group signature linker. The level of anonymity of the mechanism depends on the anonymity strength (i.e., the size of the group), whether there is an opening capability, whether there is a linking capability, how revocation is done, whether the issuer knows the private keys, and the likelihood of compromise of a private key.

Such an anonymous digital signature mechanism is defined by the specification of the following processes:

— key generation process,

— signature process,

— verification process,

— opening process (if the mechanism supports opening),

— linking process (if the mechanism supports linking), and

— revocation process.

The anonymous digital signature mechanisms using a group public key specified in this part of ISO/IEC 20008 involve a range of types of entity. Some of these entities exist in every mechanism whereas others exist only in some mechanisms. These entities are as follows:

— **Signer**: a signer is an entity that generates a digital signature. In some mechanisms, a signer role is split between two entities. For example, in direct anonymous attestation mechanisms, the signer

role is 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 with an embedded TPM).

— **Verifier**: a verifier is an entity that verifies a digital signature.

— **Group membership issuer**: a group membership issuer is an entity that issues a group membership credential to a signer. This entity exists in all the mechanisms.

— **Group membership opener**: a group membership opener is an entity who can identify the signer from a signature. This entity exists in some of the mechanisms.

— **Group signature linker**: a group signature linker is an entity that checks whether two signatures have been generated by the same signer with a linking key or a linking base. This entity exists in some of the mechanisms.

In order to use any of the mechanisms specified in this part of ISO/IEC 20008, the following requirements shall be met:

— Each entity involved in an anonymous digital signature mechanism is aware of a common set of group public parameters, which are used to compute a variety of functions in the mechanism.

— Each verifier has access to an authentic copy of the group public key.

— An authentic channel is required between a signer and a group membership issuer during the process of issuing group member signature key. This ensures that the group membership issuer is able to provide the group member signature key only to a legitimate group member.

— A collision-resistant hash function such as one of those specified in ISO/IEC 10118 shall be used.

— A robust random bit generator such as one of those specified in ISO/IEC 18031 shall be used.

— A robust prime number generator such as one of those specified in ISO/IEC 18032 shall be used.

— A robust elliptic curve generator such as one of those specified in ISO/IEC 15946-5 shall be used in some mechanisms.

6 Mechanisms with linking capability

6.1 General

This clause specifies four digital signature mechanisms with linking capability.

NOTE 1 In the literature the mechanism of 6.2 is called a list signature scheme, and the mechanisms of 6.3, 6.4 and 6.5 are called DAA schemes. The mechanisms given in 6.2, 6.4 and 6.5 are based on schemes originally specified in [9], [6], and [11], respectively, in which security proofs can also be found. The mechanism in 6.3 is based on a scheme in [3] which is a minor modification of the scheme in [4]; the associated security analysis is given in the full version of [4].

NOTE 2 For certain applications such as attestation, a message to be signed may be hashed and/or concatenated with additional information before being input to the signature process of one of the anonymous digital signature mechanisms specified in this clause.

6.2 Mechanism 1

6.2.1 Symbols

The following symbols apply in the specification of this mechanism.

— l_p, k, l_x, l_e, l_E, l_X, ε: security parameters.

— p', q', e: prime numbers.

— a, a_0, g, h, b, C_1, D, C_2, d', d_1, d_2, t', t_1, t_2, A, f, T_1, T_2, T_3, T_4, d_3, d_4, d_5, t_3, t_4, t_5: integers in QR(n).

— x', α, β: integers in $[0, 2^{lx} -1]$.

— w_1, w_2, w_3: integers in $[0, 2^{2lp} -1]$.

— $\hat{c}$, $\dot{c}$, c', c, c'', c''': k-bit integers.

— $\check{r}$: $(2l_p + 1)$-bit integer.

— t_1, $\hat{s}_1$, r', r_1, r_2: $(\varepsilon \cdot (l_x + k))$-bit integers.

— t_2, $\hat{s}_2$: $(\varepsilon \cdot (2l_p + k + 1))$-bit integers.

— x: $(l_x + 1)$-bit integer.

— r_3: $(\varepsilon \cdot (l_x + 2l_p + k + 1))$-bit integer.

— s_0, s_1, s_2, s': integers in $[-2^{lx+k}, 2^{\varepsilon(lx+k)}-1]$.

— s_3: integer in $[-2^{lx+2lp+k+1}, 2^{\varepsilon(lx+2lp+k+1)}-1]$.

— r_4, r_5: $(\varepsilon \cdot (2l_p + k))$-bit integers.

— r_9, r_{10}: $(\varepsilon \cdot (2l_p + l_e + k))$-bit integers.

— s_4, s_5: integers in $[-2^{2lp+k}, 2^{\varepsilon(2lp+k)}-1]$.

— s_9, s_{10}: integers in $[-2^{2lp+le+k}, 2^{\varepsilon(2lp+le+k)}-1]$.

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

— H_I: a hash function that outputs $(2l_p)$-bit message digest.

6.2.2 Key generation process

The key generation process has two parts: a setup process and a group membership issuing process. The setup process is executed by the group membership issuer to create the group public parameter, group public key, and group membership issuing key. The group membership issuing process is an interactive protocol running between the group membership issuer and a group member to create a unique group member signature key for the group member.

The setup process takes the following steps by the group membership issuer:

a) Choose the following parameters: l_p, k, l_x, l_e, l_E, l_X, ε.

b) Choose an RSA modulus $n = pq$ with $p = 2p' + 1$, $q = 2q' + 1$ such that p, q, p', q' are all primes and p' as well as q' have l_p bits.

c) Choose a random generator a of the group of quadratic residues modulo n by performing the following steps:

   1) Choose a random integer g in Z_n^* such that $\gcd(g+1, n) = 1$ and $\gcd(g -1, n) = 1$.

   2) Compute $a = g^2 \pmod{n}$.

d) Choose a random generator a_0 of QR(n) different from a.

e) Choose a random generator g of QR(n) different from a and a_0.

f) Choose a random generator h of QR(n) different from a, a_0 and g.

g) Choose a random generator b of QR(n) different from a, a_0, g and h.

h) The group membership issuer chooses two hash functions H: $\{0, 1\}^* \rightarrow \{0, 1\}^k$ and H_Γ: $\{0, 1\}^* \rightarrow \{0, 1\}^{2lp}$. An example of how to construct H_Γ is provided in Annex B.

i) Output the following:

— group public parameter = (l_p, k, l_x, l_e, l_E, l_X, ε),

— group public key = (n, a, a_0, g, h, b),

— group membership issuing key = (p', q').

NOTE An example of recommended parameters is provided in Annex C.2.

The group membership issuing process may require a secure and authentic channel between the member and the group membership issuer to prevent the group membership credential from being observed by an eavesdropper. How to establish such a channel is out scope of this mechanism. The group membership issuing process is as follows:

a) The group member chooses a random integer $x' \in [0, 2^{lx}-1]$.

b) The member chooses a random integer $\check{r} \in [0, 2n-1]$.

c) The member computes $C_1 = g^{x'}h^{\check{r}} \pmod n$.

d) The member generates a proof of knowledge U of the representation (x', $\check{r}$) of C_1 in the bases g and h by performing the following steps:

1) The member chooses a random integer $t_1 \in [0, 2^{\varepsilon(lx+k)}-1]$.

2) The member chooses a random integer $t_2 \in [0, 2^{\varepsilon(2lp+k+1)}-1]$.

3) The member computes $D = g^{t1}h^{t2} \pmod n$.

4) The member computes $\hat{c} = H(g \,||\, h \,||\, C_1 \,||\, D)$.

5) The member computes $\hat{s}_1 = t_1 - \hat{c}\,x'$.

6) The member computes $\hat{s}_2 = t_2 - \hat{c}\,\check{r}$.

7) $U = (\hat{c}, \hat{s}_1, \hat{s}_2)$.

e) The member sends C_1 and U to the group membership issuer.

f) The group membership issuer receives C_1 and U from the member.

g) The group membership issuer verifies that C_1 belongs to QR(n) by performing the following step:

1) The group membership issuer checks that $(C_1|p) = 1$ and that $(C_1|q) = 1$. If either of these verifications fails, the group membership issuer outputs Reject and stops.

h) The group membership issuer verifies the proof of knowledge U by performing the following steps:

1) The group membership issuer computes $D' = g^{\hat{s}1}h^{\hat{s}2}C_1^{\hat{c}} \pmod n$.

2) The group membership issuer computes $\dot{c} = H(g \,||\, h \,||\, C_1 \,||\, D')$.

3) The group membership issuer checks that $\dot{c} = \hat{c}$, $\hat{s}_1$ belongs to $[-2^{lx+k}, 2^{\varepsilon(lx+k)}-1]$ and $\hat{s}_2$ belongs to $[-2^{2lp+k+1}, 2^{\varepsilon(2lp+k+1)}-1]$. If any of these verifications fails, the group membership issuer outputs Reject and stops.

i) The group membership issuer chooses a random odd integer $\alpha \in [0, 2^{lx}-1]$.

j) The group membership issuer chooses a random integer $\beta \in [0, 2^{lx}-1]$.

k) The group membership issuer sends α and β to the member.

l) The member receives α and β from the group membership issuer.

m) The member computes $x = 2^{lX} + (\alpha x' + \beta \pmod{2^{lx}})$.

n) The member computes $C_2 = a^x \pmod{n}$.

o) The member computes $v = (\alpha x' + \beta) \mid 2^{lx}$.

p) The member generates a proof of knowledge V of the discrete logarithm x of C_2 in base a by performing the following steps:

1) The member chooses a random integer $r' \in [0, 2^{\varepsilon(lx+k)}-1]$.

2) The member computes $d' = a^{r'} \pmod{n}$.

3) The member computes $c' = H(a \,||\, g \,||\, C_2 \,||\, d')$.

4) The member computes $s' = r' - c'(x - 2^{lX})$.

5) The member set $V = (c', s')$.

q) The member generates a proof of knowledge W by performing the following steps:

1) The member chooses a random integer $r_1 \in [0, 2^{\varepsilon(lx+k)}-1]$.

2) The member chooses a random integer $r_2 \in [0, 2^{\varepsilon(lx+k)}-1]$.

3) The member chooses a random integer $r_3 \in [0, 2^{\varepsilon(lx+2lp+k+1)}-1]$.

4) The member computes $d_1 = a^{r1} \pmod{n}$.

5) The member computes $d_2 = g^{r1}(gl)^{r2}h^{r3} \pmod{n}$ where $l = 2^{lx}$.

6) The member computes $c = H(a \,||\, g \,||\, h \,||\, C_1 \,||\, C_2 \,||\, d_1 \,||\, d_2)$.

7) The member computes $s_1 = r_1 - c(x - 2^{lX})$.

8) The member computes $s_2 = r_2 - cv$.

9) The member computes $s_3 = r_3 - c\alpha\check{r}$.

10) The member sets $W = (c, s_1, s_2, s_3)$.

r) The member sends C_2, V and W to the group membership issuer.

s) The group membership issuer receives C_2, V and W from the member.

t) The group membership issuer checks that C_2 belongs to QR(n) by performing the following step:

1) The group membership issuer checks that $(C_2|p) = 1$ and that $(C_2|q) = 1$. If any of these verifications fails, the group membership issuer outputs Reject and stops.

u) The group membership issuer verifies the proof of knowledge V by performing the following steps:

1) The group membership issuer computes $s_0 = s' - c' 2^{lX}$.

2) The group membership issuer computes $t' = C_2{}^{c'} a^{s0} \pmod{n}$.

3) The group membership issuer computes $c'' = H(a \,||\, g \,||\, C_2 \,||\, t')$.