INTERNATIONAL STANDARD

ISO/IEC 20009-2

First edition
2013-12-01

Information technology — Security techniques — Anonymous entity authentication —

Part 2:
Mechanisms based on signatures using a group public key

Technologies de l'information — Techniques de sécurité - Authentification anonyme d'entité —

Partie 2: Mécanismes fondés sur des signatures numériques utilisant une clé publique de groupe

Reference number
ISO/IEC 20009-2:2013(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 .... **iv**
Introduction .... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **3**
5 General model and requirements **4**
6 Key generation process **5**
7 Mechanisms without an online TTP **6**
7.1 Introduction 6
7.2 Unilateral anonymous authentication 7
7.3 Mutual anonymous authentication 9
7.4 Unilateral-anonymous mutual authentication 12
7.5 Mutual anonymous authentication with binding-property 15
7.6 Unilateral-anonymous mutual authentication with binding-property 21
8 Mechanisms involving an online TTP **28**
8.1 Introduction 28
8.2 Unilateral anonymous authentication 28
8.3 Mutual anonymous authentication 31
8.4 Unilateral-anonymous mutual authentication 35
9 The group membership opening process **44**
9.1 General 44
9.2 The evidence evaluation process 45
10 The group signature linking process **45**
10.1 General 45
10.2 Linking process with opener 45
10.3 Linking process with linking key 46
10.4 Linking process with linking base 46
Annex A (normative) **Object identifiers** **47**
Annex B (informative) **Information on mechanisms with binding-property** **49**
Bibliography **51**

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 20009-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 20009 consists of the following parts, under the general title *Information technology — Security techniques — Anonymous entity authentication*:

— *Part 1: General*

— *Part 2: Mechanisms based on signatures using a group public key*

Mechanisms based on blind signatures and *Mechanisms based on weak secrets* will form the subjects of future Parts 3 and 4, respectively.

Further parts may follow.

Introduction

Anonymous entity authentication is a special type of entity authentication. In an anonymous entity authentication mechanism, given a message that was generated during the authentication protocol, an unauthorized entity cannot discover the identifier of the entity being authenticated (the claimant). At the same time, an authorized verifier can obtain assurance that the claimant is authentic. However, even an authorized verifier may not be authorized to learn the identifier of the entity being authenticated.

The anonymous entity authentication mechanisms specified in this part of ISO/IEC 20009 are based on anonymous signatures using a group public key, discussed in ISO/IEC 20008-2. An anonymous signature using a group public key is sometimes simply known as a group signature. A group signature has the following properties.

- Only group members are able to correctly sign messages.
- The verifier can verify that it is a valid group signature, but cannot discover which group member generated it.
- Optionally, the signature can be "linked" or "opened".

The anonymous entity authentication mechanisms specified in this part of ISO/IEC 20009 involve the following basic operations.

- An entity (verifier) which wants to authenticate another entity (claimant) interacts with the claimant.
- The claimant sends a token (and optionally a group public key certificate) to the verifier.
- The verifier confirms the validity of the provided token (and optionally the group public key certificate).

One of the major differences between a (conventional) entity authentication mechanism based on (conventional) digital signatures and an anonymous entity authentication mechanism based on signatures using a group public key is the nature of the digital signature scheme used to produce tokens and to provide confirmation of messages that were generated during the authentication protocol. Another difference is that, for an anonymous authentication mechanism, the claimant belongs to a group, and authentication is conducted with respect to this group. Authentication mechanisms require associated methods to manage the relationship between an entity and a group; for example, how an entity joins the group, how its activity can be linked, and how it can be later identified must all be specified. Thus, this standard specifies methods for issuing, linking and opening.

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 ensured 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, 305-700, KOREA
- China IWNCOMM Co., LTD.
  A201,QinFeng Ge, Xi'an Software Park, No.68 KeJi 2nd Road,
  Xi'an Hi-tech Industrial Development Zone, Shaanxi, P.R.China 710075

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 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 online 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 entity authentication —

Part 2:
Mechanisms based on signatures using a group public key

1 Scope

This part of ISO/IEC 20009 specifies anonymous entity authentication mechanisms based on signatures using a group public key in which a verifier verifies a group signature scheme to authenticate the entity with which it is communicating, without knowing this entity's identity.

This part of ISO/IEC 20009 provides

- a general description of an anonymous entity authentication mechanism based on signatures using a group public key;
- a variety of mechanisms of this type.

This part of ISO/IEC 20009 describes

- the group membership issuing processes;
- anonymous authentication mechanisms without an online Trusted Third Party (TTP);
- anonymous authentication mechanisms involving an online TTP.

Furthermore, this part of ISO/IEC 20009 also specifies

- the group membership opening process (optional);
- the group signature linking process (optional).

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

ISO/IEC 20008-2, *Information technology — Security techniques — Anonymous digital signature — Part 2: Mechanisms using a group public key*

ISO/IEC 20009-1, *Information technology — Security techniques — Anonymous entity authentication — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20008-1, ISO/IEC 20009-1, and the following apply.

3.1
binding-property
property providing assurance for binding between the messages of a communicating entity

3.2
certification authority
entity trusted to create and assign public key certificates

[SOURCE: ISO/IEC 11770-1:2010]

3.3
ephemeral key pair
asymmetric key pair consisting of an ephemeral public key and an ephemeral private key that are used as a temporary key and are unique for each execution of a cryptographic scheme

3.4
group public key certificate
group public key information of a group signed by the group public key certification authority

3.5
group public key certification authority
entity trusted to create and assign group public key certificates

3.6
group public key information
information containing at least the group's identifier and group public key, but which can include other static information regarding the group public key certification authority, the group, restrictions on key usage, the validity period, or the involved algorithms

3.7
key derivation function
function that outputs one or more shared secrets, for use as keys, given shared secrets and other mutually known parameters as input

[SOURCE: ISO/IEC 11770-3:2008]

3.8
local linking capability
linking capability with a feature that two or more signatures from same anonymous user are linked only by a specific group signature linker with linking key, but other entities cannot link the signatures

3.9
message authentication code (MAC)
string of bits which is the output of a MAC algorithm

[SOURCE: ISO/IEC 9797-1:2011]

3.10
message authentication code (MAC) algorithm
algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits satisfying the following two properties:

— for any key and any input string, the function can be computed efficiently;

— for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the i th input string may have been chosen after observing the value of the first $i - 1$ function values

[SOURCE: ISO/IEC 9797-1:2011]

3.11
public key certificate
public key information of an entity signed by the certification authority

[SOURCE: ISO/IEC 11770-1:2010]

3.12
public key information
information containing at least the entity's distinguishing identifier and public key, but which can include other static information regarding the certification authority, the entity, restrictions on key usage, the validity period, or the involved algorithms

[SOURCE: ISO/IEC 11770-1:2010]

4 Symbols and abbreviated terms

For the purposes of this part of ISO/IEC 20009, the following symbols and abbreviations apply.

A, B	distinguishing identifier of entity A or B
$Cert_A$, $Cert_B$	public key certificate of entity A or B
$Cert_G$	group public key certificate of the group G
G, G'	distinguishing identifier of the group G or G'
$\boldsymbol{G}$	cyclic group of order q in which the decisional Diffie-Hellman (DDH) problem is hard
g	generator of $\boldsymbol{G}$
$gsS_{XG}(m)$	anonymous signature using a group public key created by entity X applying one of group signature mechanisms specified in ISO/IEC 20008-2 on message-to-be-signed m using the group member signature key S_{XG}
kdf	key derivation function
I_G	identity of group G which is either G or $Cert_G$
I_X	identity of entity X which is either X or $Cert_X$
m	message-to-be-signed
MAC	Message Authentication Code
MAC	output value of a MAC algorithm
$mac_K(M)$	MAC algorithm using the secret key K and an arbitrary data string M
N_X	sequence number issued by entity X
P_A, P_B	public key of entity A or B
P_G	group public key of a group G
q	prime number
Res_A, Res_B	result of verifying a public key or a public key certificate of entity A or B
Res_G	result of verifying a group public key or a group public key certificate for the group G
R_X	random number issued by entity X

S_{XG} group member signature key associated with entity X where entity X is a member of the group G

$sS_X(m)$ digital signature created by entity X on message m using the private signature key of entity X

TP distinguishing identifier of a TTP

TTP Trusted Third Party

T_X time stamp issued by entity X

Z_q the set of integers between $[0, q - 1]$

|| Y || Z is used to mean the result of the concatenation of data items Y and Z in the order specified. In cases where the result of concatenating two or more data items is input to a function as part of one of the mechanisms specified in this document, 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]

Data items that are optional are shown in square brackets.

5 General model and requirements

Clause 5 specifies the general model and requirements for the anonymous authentication mechanisms specified in this part of ISO/IEC 20009.

An anonymous entity authentication mechanism based on signatures using a group public key involves a set of group members. Every group must have an associated group membership issuer. A group may also have a group opener if it is necessary to allow opening of a group signature that was generated during the authentication protocol to reveal its claimant. A group may also have a linker if it is necessary to link two group signatures that were generated by the same claimant for authentication purposes. The anonymity strength of the mechanism depends on the number of group members. An anonymous entity authentication mechanism is defined by the specification of the following processes.

- Key generation process.
- Anonymous entity authentication process.
- Opening process (if the mechanism supports opening).
- Linking process (if the mechanism supports linking).

As defined below, entities of a variety of types can be involved in the mechanisms specified in this part of ISO/IEC 20009. While some are involved in all mechanisms, others only participate in some mechanisms. In this part of ISO/IEC 20009, if a mechanism supports opening or linking, then the operation of the associated processes follows those of the group signature scheme in use, as specified in ISO/IEC 20008-2.

- **Claimant:** an entity to be authenticated in such a way that the claimant's identity is not revealed. In this part of ISO/IEC 20009, a claimant plays the role of a signer in group signature schemes which are specified in ISO/IEC 20008-2.

NOTE In some mechanisms, the role of a claimant is split between multiple entities. For example, the Direct Anonymous Attestation (DAA) mechanisms involve a principal claimant with limited computational and storage capability, e.g. a trusted platform module (TPM), and an assistant claimant with more computational power but less security tolerance, e.g. an ordinary computer platform (namely the Host in which the TPM is embedded).

— **Verifier:** an entity verifying the correctness of the claimant, which does not learn the claimant's identity.

— **Issuer:** an entity issuing a group membership credential to a claimant. This entity exists in all the mechanisms specified in ISO/IEC 20008-2.

— **Opener:** an entity capable of determining the claimant that created a group signature that was generated during the authentication protocol. This entity exists in some of the mechanisms specified in ISO/IEC 20008-2. In some mechanisms, the group membership issuer and the group membership opener are the same entity.

— **Linker:** an entity capable of determining whether or not two group signatures, generated for authentication purposes, were created by the same claimant. This entity exists in some of the mechanisms specified in ISO/IEC 20008-2. In some mechanisms, the linker is also the verifier. The number of linkers in an anonymous entity authentication mechanism is not fixed.

It is required that each entity involved in an anonymous entity authentication mechanism is aware of a common set of group public parameters, which are used to compute a variety of functions in the mechanism.

The 24 authentication mechanisms specified in this part of ISO/IEC 20009 have the following intended uses. If an online TTP is not required or not available, then a mechanism in Clause 7 should be used. Of the 16 mechanisms in Clause 7, mechanisms 1-8 do not have the binding-property, whereas mechanisms 9-16 do have this property. If a mechanism using an online TTP is needed and available, then a mechanism in Clause 8 should be used. Both Clauses 7 and 8 specify mechanisms providing unilateral anonymous authentication, mutual anonymous authentication and unilateral-anonymous mutual authentication, and offer options with varying number of passes.

The revocation process is used to revoke a user and to check whether a user has been revoked. Details of the process depend on the anonymous digital signature scheme used in creating the token for anonymous authentication. A general model for the revocation process is specified in ISO/IEC 20008-1, and the operational processes of individual anonymous signature schemes using a group public key are specified in ISO/IEC 20008-2.

6 Key generation process

The key generation process includes key generation algorithms that create 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. Details of the key generation algorithms are outside the scope of this part of ISO/IEC 20009.

The key generation process also includes a group membership issuing process. The group membership issuing process operates between a group member and an issuer, and involves the creation of a group member signature key.

To prevent the group membership credential from being observed by an eavesdropper and to ensure that the group membership credential is only provided to a legitimate group member, a secure and authentic channel is required between a group member (as a claimant) and an issuer. This standard does not specify how the group issuer authenticates a group member.

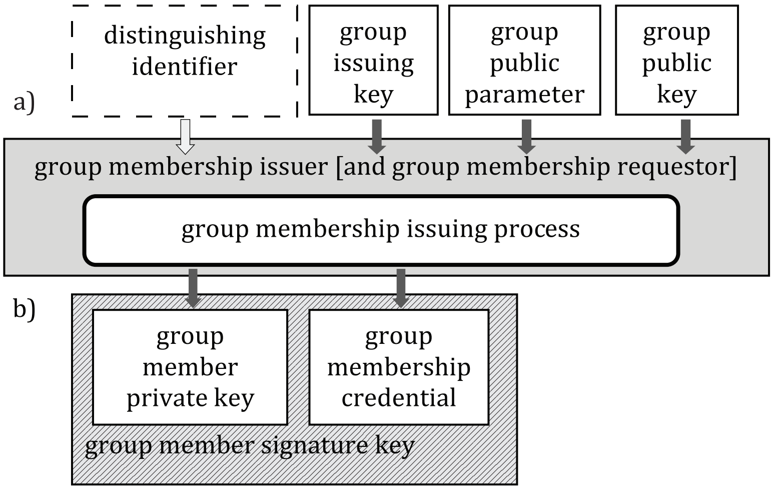
a)
distinguishing identifier
group issuing key
group public parameter
group public key
group membership issuer [and group membership requestor]
group membership issuing process
b)
group member private key
group membership credential
group member signature key

Figure 1 — A group membership issuing process

Key generation can be divided into steps a) and b), as shown in Figure 1 and described below.

a) The group membership issuer takes the group issuing key, group public key, group public parameter and optionally the distinguishing identifier as input. In this step, a group membership issuer might interoperate with a group member.

b) The group membership issuing process outputs a group member signature key.

7 Mechanisms without an online TTP

7.1 Introduction

Clause 7 specifies anonymous entity authentication mechanisms without an online TTP. Mechanisms specified in Clause 7 use the group public key certificate or some other means to enable the validity of the group public key to be verified. Extensions of these mechanisms to cover the opening and linking processes are specified in Clauses 9 and 10 respectively.

The specified entity authentication mechanisms make use of time variant parameters such as time stamps, sequence numbers or random numbers (see Annex B of ISO/IEC 9798-1:2010[3] and Note 1 below).

In this part of ISO/IEC 20009, tokens sometimes have the following form:

Token = $X_1 \| X_2 \| \ldots \| X_i \| gsS_{XG}(Y_1 \| Y_2 \| \ldots \| Y_j)$

In a unilateral-anonymous mutual authentication, a digital signature $sS_X(Y_1 \| Y_2 \| \ldots \| Y_j)$ could be substituted for the group signature $gsS_{XG}(Y_1 \| Y_2 \| \ldots \| Y_j)$.

In both a mutual anonymous authentication with the binding-property and a unilateral-anonymous mutual authentication with the binding-property, a MAC could be additionally concatenated or a MAC could be substituted for the group signature $gsS_{XG}(Y_1 \| Y_2 \| \ldots \| Y_j)$.

In this part of ISO/IEC 20009, the term “message-to-be-signed” refers to the string “$Y_1 \| Y_2 \| \ldots \| Y_j$” used as input to the group signature scheme, and the term “message” refers to the string “$X_1 \| X_2 \| \ldots \| X_i$”. Essential parts of $X_1 \| X_2 \| \ldots \| X_i$ and $Y_1 \| Y_2 \| \ldots \| Y_j$ should be the same; other parts may differ depending on the group signature schemes and specific applications.

If information contained in the message-to-be-signed of the token can be recovered from the group signature, then it need not be contained in the message of the token.

If information contained in the text field of the message-to-be-signed of the token cannot be recovered from the group signature, then it shall be contained in the unsigned text field of the token.

If information in the message-to-be-signed of a token sent by the claimant to the verifier is already known to the verifier (e.g. a random number), then it need not be contained in the message of the token.

All text fields specified in the mechanisms specified in this part of ISO/IEC 20009 are available for use in applications outside the scope of this part of ISO/IEC 20009 (they may be empty). Their relationship and contents depend upon the specific application. See Annex A of ISO/IEC 9798-3:1998[4] for information on the use of text fields.

NOTE 1 The security issues associated with the signing by one entity of a data block which has been manipulated by a second entity for some ulterior motive can be mitigated by the first entity including its own random number in the data block which it signs. In this case, it is the unpredictability of the random number which prevents the signing of completely pre-defined data.

NOTE 2 As the distribution of group public key certificates is outside the scope of this part of ISO/IEC 20009, the sending of group public key certificates is optional in all mechanisms, except the mechanisms involving an online TTP specified in Clause 8.

7.2 presents unilateral anonymous authentication mechanisms that provide one entity with assurance of the legitimacy of the other entity, but not vice versa. 7.3 presents mutual anonymous authentication mechanisms that provide both entities with assurance of the legitimacy of the other entity. 7.4 provides unilateral-anonymous mutual authentication mechanisms that provide anonymous entity authentication in one direction and entity authentication in the other direction.

The three-pass authentication and two-pass parallel authentication protocols in 7.3 and 7.4 may be subject to a misbinding attack (see[11]). When the challenge and Token messages are not bound together, it is possible for one entity to send the challenge message and another entity in the same group to send the Token message. More information about the misbinding attack and the binding-property is provided in Annex B.

To mitigate the misbinding attack, 7.5 and 7.6 provide eight mechanisms with the binding-property for both three-pass and two-pass parallel authentication protocols.

7.2 Unilateral anonymous authentication

7.2.1 General

Unilateral anonymous authentication means that only one of the two entities, the Claimant (entity A in the group G), is authenticated by use of the mechanism and that the identity of the authenticated entity is anonymous to the other entity, the Verifier (entity B).

7.2.2 Mechanism 1 — One-pass unilateral anonymous authentication

In this mechanism, entity A in the group G initiates the authentication protocol with entity B, and uniqueness/timeliness is controlled by generating and checking a time stamp or sequence number (see Annex B of ISO/IEC 9798-1:2010[3]).

The authentication mechanism is illustrated in Figure 2.

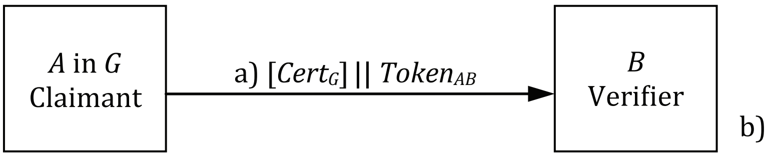

Figure 2 — One-pass unilateral anonymous authentication

The form of the token ($Token_{AB}$), sent by the claimant A to the verifier B is:

$Token_{AB} = T_A$ or $N_A \,||\, B \,||\, [Text_2] \,||\, gsS_{AG}(T_A$ or $N_A \,||\, B \,||\, [Text_1])$

The claimant A uses either a time stamp T_A or a sequence number N_A as the time variant parameter. The choice depends on the technical capabilities of the claimant and the verifier as well as on the environment. The signature gsS_{AG} is a group signature created using one of the group signature mechanisms specified in ISO/IEC 20008-2. $Cert_G$ is a group public key certificate for the group public key of a group G.

NOTE 1 The inclusion of identifier B in the message-to-be-signed of $Token_{AB}$ is necessary to prevent the token from being accepted by anyone other than the intended verifier.

NOTE 2 In general, $Text_2$ is not authenticated by this process.

NOTE 3 One application of this mechanism could be key distribution (see Annex A of ISO/IEC 9798-1:2010[3]).

The mechanism is performed as follows:

a) A sends $Token_{AB}$ and optionally $Cert_G$ to B.

b) On receipt of the message containing $Token_{AB}$, B performs the following steps:

   1) It ensures that it is in possession of the valid group public key of the group G either by verifying the group public key certificate of G or by some other means.

   2) It verifies $Token_{AB}$ by verifying the group signature of A contained in the token, by checking the time stamp or sequence number, and by checking that the value of the identifier field (B) in the message-to-be-signed of $Token_{AB}$ is equal to entity B's identifier.

7.2.3 Mechanism 2 — Two-pass unilateral anonymous authentication

In this mechanism, entity A in G is authenticated by entity B which initiates the process and uniqueness/timeliness is controlled by generating and checking a random number R_B (see Annex B of ISO/IEC 9798-1:2010[3]).

The authentication mechanism is illustrated in Figure 3.

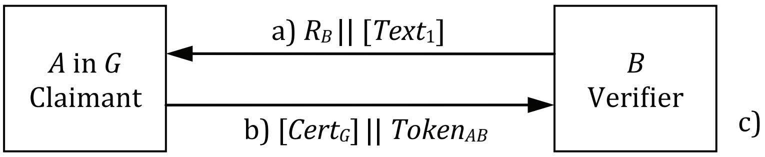

Figure 3 — Two-pass unilateral anonymous authentication

The form of the token ($Token_{AB}$), sent by the claimant A to the verifier B is:

$Token_{AB} = R_A \,||\, R_B \,||\, [B] \,||\, [Text_3] \,||\, gsS_{AG}(R_A \,||\, R_B \,||\, [B] \,||\, [Text_2])$

The inclusion of identifier B in $Token_{AB}$ is optional. It depends on the environment in which this authentication mechanism is used.

NOTE 1 The inclusion of the optional identifier B in the message-to-be-signed of $Token_{AB}$ can prevent the token from being accepted by anyone other than the intended verifier (e.g. as might occur in a person-in-the-middle attack).

NOTE 2 The inclusion of the random number R_A in the signed part of $Token_{AB}$ prevents B from obtaining the group signature of A on data chosen by B prior to the start of the authentication mechanism. This measure may be required, for example, when the same group public key is used by A for purposes other than entity authentication or by another group member.

The mechanism is performed as follows:

a) B sends a random number R_B and, optionally, a text field $Text_1$ to A.

b) *A* sends $Token_{AB}$ and, optionally, $Cert_G$ to *B*.

c) On receipt of the message containing $Token_{AB}$, *B* performs the following steps:

  1) It ensures that it is in possession of the valid group public key of *G* either by verifying the group public key certificate of *G* or by some other means.

  2) It verifies $Token_{AB}$ by checking the group signature of *A* contained in the token, by checking that the random number R_B, sent to *A* in step a), agrees with the random number contained in the message-to-be-signed of $Token_{AB}$, and by checking that the value of the identifier field (*B*) in the message-to-be-signed of $Token_{AB}$, if present, is equal to *B*'s identifier.

7.3 Mutual anonymous authentication

7.3.1 General

Mutual anonymous authentication means that the two communicating entities are authenticated to each other, and that the identities of the two entities are anonymous to each other.

The two mechanisms described in 7.2.2 and 7.2.3 are extended in 7.3.2 and 7.3.3, respectively, to achieve mutual authentication. This is achieved by transmitting one additional message.

The mechanism specified in 7.3.4 uses four steps which, however, need not all be sent consecutively. As a result it may be possible to reduce the time taken to perform the authentication process.

7.3.2 Mechanism 3 — Two-pass mutual anonymous authentication

In this mechanism, entity *A* in the group *G* initiates the authentication protocol with entity *B* in the group *G'* and uniqueness/timeliness is controlled by generating and checking time stamps or sequence numbers (see Annex B of ISO/IEC 9798-1:2010[3]). Entity *A* knows the identity of the group *G'*.

The authentication mechanism is illustrated in Figure 4.

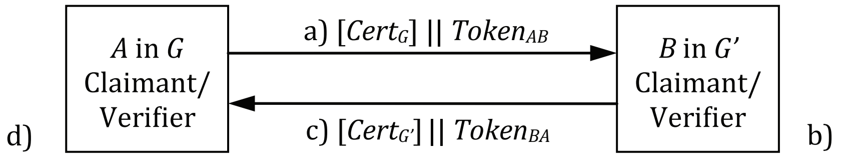

Figure 4 — Two-pass mutual anonymous authentication

The form of the token ($Token_{AB}$), sent by *A* to *B*, is:

$Token_{AB} = T_A$ or $N_A \,||\, G' \,||\, [Text_2] \,||\, gsS_{AG}(T_A$ or $N_A \,||\, G' \,||\, [Text_1])$

The form of the token ($Token_{BA}$), sent by *B* to *A*, is:

$Token_{BA} = T_B$ or $N_B \,||\, G \,||\, [Text_4] \,||\, gsS_{BG'}\,(T_A$ or $N_A \,||\, G \,||\, [Text_3])$

The choice of using either time stamps or sequence numbers in this mechanism depends on the technical capabilities of the claimant and the verifier as well as on the environment.

NOTE 1 The inclusion of identifiers *G* and *G'* in the message-to-be-signed of $Token_{BA}$ and $Token_{AB}$, respectively, is necessary to prevent the tokens from being accepted by anyone other than a member of intended group.

The mechanism is performed as follows:

a) *A* sends $Token_{AB}$ and, optionally $Cert_G$ to *B*.