INTERNATIONAL STANDARD

ISO/IEC 9798-3

First edition
1993-11-15

Information technology — Security techniques — Entity authentication mechanisms —

Part 3:
Entity authentication using a public key algorithm

Technologies de l'information — Techniques de sécurité — Mécanismes d'authentification d'entité —

Partie 3: Authentification d'entité utilisant un algorithme à clé publique

ISO IEC

Reference number
ISO/IEC 9798-3:1993(E)

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. 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.

International Standard ISO/IEC 9798-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication mechanisms*:

- *Part 1: General model*
- *Part 2: Entity authentication using symmetric techniques*
- *Part 3: Entity authentication using a public key algorithm*

Further parts may follow.

Annexes A, B, C and D of this part of ISO/IEC 9798 are for information only.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Information technology - Security techniques - Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using a public key algorithm. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities. A digital signature is used to verify the identity of an entity. A trusted third party may be involved.

The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time.

If a time stamp or a sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three or four passes (depending on the mechanism employed) are required to achieve mutual authentication.

2 Normative reference

The following standard contains provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the edition indicated was valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 9798-1: 1991, *Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model.*

3 Definitions and notation

For the purposes of this part of ISO/IEC 9798 the definitions and notation described in ISO/IEC 9798-1 apply.

4 Requirements

In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identiy by demonstrating its knowledge of its secret signature key. This is achieved by the entity using its secret signature key to sign specific data. The signature can be verified by anyone using the entity's public verification key.

The authentication mechanisms have the following requirements. If any of these is not met then the authentication process may be compromised or it cannot be implemented.

a) A verifier shall possess the valid public key of the claimant.

b) A claimant shall have a secret signature key known and used only by itself.

> NOTE — One way of obtaining a valid public key is by means of a certificate (see annex B). The generation, distribution, and revocation of certificates are outside the scope of this part of ISO/IEC 9798. There may exist a trusted third party for this purpose. Another way of obtaining a valid public key is by trusted courier.

5 Mechanisms

The specified entity authentication mechanisms make use of time variant parameters such as time stamps, sequence numbers or random numbers (see annex C).

In this part of ISO/IEC 9798, given a token defined as

$$\text{Token} = X_1 || \cdots || X_i || sS_A(Y_1 || \cdots || Y_j)$$

the "signed data" refers to "$Y_1||\cdots||Y_j$" used as input to the signature scheme and the "unsigned data" refers to "$X_1||\cdots||X_i$".

If information contained in the signed data of the token can be recovered from the signature, then it need not be contained in the unsigned data of the token (see, for example, ISO/IEC 9796).

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

All text fields specified in the following mechanisms are available for use in applications outside the scope of this part of ISO/IEC 9798 (they may be empty). Their relationship and contents depend upon the specific application. See annex A for information on the use of text fields.

NOTE — As the distribution of certificates is outside the scope of this part of ISO/IEC 9798, the sending of certificates is optional in all mechanisms.

5.1 Unilateral authentication

Unilateral authentication means that only one of the two entities is authenticated by use of the mechanism.

5.1.1 One pass authentication

In this authentication mechanism the claimant A initiates the process and is authenticated by the verifier B. Uniqueness / timeliness is controlled by generating and checking a time stamp or a sequence number (see annex C).

The authentication mechanism is illustrated in figure 1.

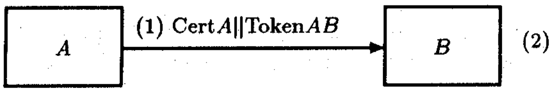

Figure 1

The form of the token (TokenAB), sent by the claimant A to the verifier B is:

$$\text{Token}AB = \substack{T_A\\N_A}||B||\text{Text2}||sS_A\left(\substack{T_A\\N_A}||B||\text{Text1}\right),$$

where the claimant A uses either a sequence number N_A or a time stamp T_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.

NOTES

1 The inclusion of the identifier B in the signed data of TokenAB is necessary to prevent the token from being accepted by anyone other than the intended verifier.

2 In general, Text2 is not authenticated by this process.

3 One application of this mechanism could be key distribution (see annex A).

(1) A sends TokenAB and, optionally, its certificate to B.

(2) On receipt of the message containing TokenAB, B performs the following steps:

  (i) It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.

  (ii) It verifies TokenAB by checking the time stamp or the sequence number, by verifying the signature of A contained in the token and by checking that the value of the identifier field (B) in the signed data of TokenAB is equal to entity B's distinguishing identifier.

5.1.2 Two pass authentication

In this authentication mechanism the claimant A is authenticated by the verifier B who initiates the process. Uniqueness / timeliness is controlled by generating and checking a random number R_B (see annex C).

The authentication mechanism is illustrated in figure 2.

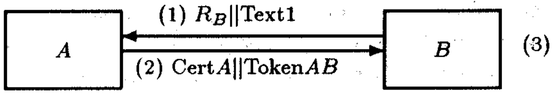

Figure 2

The form of the token (TokenAB), sent by the claimant A to the verifier B is:

$$\text{Token}AB = R_A||R_B||B||\text{Text3}||sS_A\,(R_A||R_B||B||\text{Text2}).$$

The inclusion of the parameter B in TokenAB is optional. It depends on the environment in which this authentication mechanism is used.

NOTE — The random number R_A is present in Token AB to prevent B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This prevention may be required, for example, when the same key is used by A for other purposes in addition to entity authentication.

(1) B sends a random number R_B and, optionally, a text field Text1 to A.

(2) A sends TokenAB and, optionally, its certificate to B.

(3) On receipt of the message containing TokenAB, B performs the following steps:

(i) It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.

(ii) It verifies TokenAB by checking the signature of A contained in the token and by checking that the random number R_B, sent to A in step (1), agrees with the random number contained in the signed data of TokenAB.

5.2 Mutual authentication

Mutual authentication means that the two communicating entities are authenticated to each other by use of the mechanism.

The two mechanisms described in 5.1.1 and 5.1.2 are extended in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. This is done by transmitting one further message resulting in two additional steps.

The mechanism specified in 5.2.3 uses four messages which, however, need not all be sent consecutively. In this way the authentication process may be speeded up.

5.2.1 Two pass authentication

In this authentication mechanism uniqueness / timeliness is controlled by generating and checking time stamps or sequence numbers (see annex C).

The authentication mechanism is illustrated in figure 3.

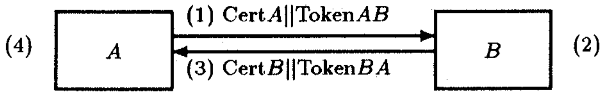

Figure 3

The form of the token (TokenAB), sent by A to B, is identical to that specified in 5.1.1.

$$\text{Token}AB = \substack{T_A \\ N_A}\,||B||\text{Text2}||sS_A\left(\substack{T_A \\ N_A}\,||B||\text{Text1}\right).$$

The form of the token (TokenBA), sent by B to A, is:

$$\text{Token}BA = \substack{T_B \\ N_B}\,||A||\text{Text4}||sS_B\left(\substack{T_B \\ N_B}\,||A||\text{Text3}\right).$$

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 A and B in the signed data of TokenBA and TokenAB, respectively, is necessary to prevent the tokens from being accepted by anyone other than the intended verifier.

Steps (1) and (2) are identical to those specified in 5.1.1, one pass authentication.

(3) B sends TokenBA and, optionally, its certificate to A.

(4) The message in step (3) is handled in a manner analogous to step (2) of 5.1.1.

NOTE 2 — The two messages of this mechanism are not bound together in any way, other than implicitly by timeliness; the mechanism involves independent use of mechanism 5.1.1 twice. If it is desired to bind these messages further, appropriate use could be made of text fields (see annex A).

5.2.2 Three pass authentication

In this authentication mechanism uniqueness / timeliness is controlled by generating and checking random numbers (see annex C).

The authentication mechanism is illustrated in figure 4.

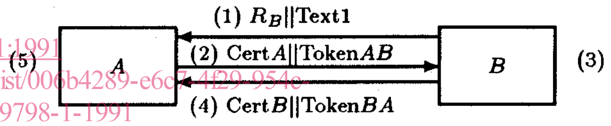

Figure 4

The tokens are of the following form:

$$\text{Token}AB = R_A||R_B||B||\text{Text3}||sS_A\,(R_A||R_B||B||\text{Text2}),$$
$$\text{Token}BA = R_B||R_A||A||\text{Text5}||sS_B\,(R_B||R_A||A||\text{Text4}).$$

The inclusion of the parameter B in TokenAB and the inclusion of the parameter A in TokenBA are optional. They depend on the environment in which this authentication mechanism is used.

NOTE — The random number R_A is present in TokenAB to prevent B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This prevention may be required, for example, when the same key is used by A for other purposes in addition to entity authentication. For similar reasons the random number R_B is present in TokenBA. Furthermore, checking that this random number is the same as the random number in the first message is necessary for security considerations.

(1) B sends a random number R_B and, optionally, a text field Text1 to A.

(2) A sends TokenAB and, optionally, its certificate to B.

(3) On receipt of the message containing TokenAB, B performs the following steps:

(i) It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.

(ii) It verifies TokenAB by checking the signature of A contained in the token and by checking that the random number R_B, sent to A in step (1), agrees with the random number contained in the signed data of TokenAB.

(4) B sends TokenBA and, optionally, its certificate to A.

(5) On receipt of the message containing TokenBA, A analogously performs steps (i) and (ii) listed under (3). In addition, A checks that the random number R_B contained in the signed data of TokenBA is equal to the random number R_B received in step (1).

5.2.3 Two pass parallel authentication

In this mechanism authentication is carried out in parallel. Uniqueness / timeliness is controlled by generating and checking random numbers (see annex C).

The authentication mechanism is illustrated in figure 5.

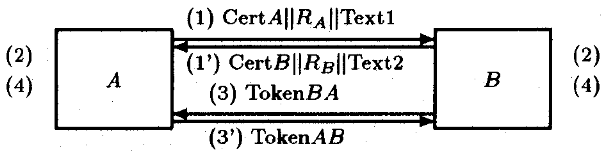

Figure 5

The tokens are similar to those of 5.1.2:

$$\text{Token}AB = R_A||R_B||B||\text{Text4}||sS_A\ (R_A||R_B||B||\text{Text3}),$$
$$\text{Token}BA = R_B||R_A||A||\text{Text6}||sS_B\ (R_B||R_A||A||\text{Text5}).$$

The inclusion of the parameter B in TokenAB and the inclusion of the parameter A in TokenBA are optional. They depend on the environment in which this authentication mechanism is used.

NOTE 1 — The random number R_A is present in TokenAB to prevent B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This prevention may be required, for example, when the same key is used by A for other purposes in addition to entity authentication. For similar reasons the random number R_B is present in TokenBA.

(1) A sends R_A and, optionally, its certificate and a text field Text1 to B.

(1') B sends R_B and, optionally, its certificate and a text field Text2 to A.

(2) A and B ensure that they are in possession of a valid public key of the other entity either by verifying the respective certificate or by some other means.

(3) B sends TokenBA to A.

(3') A sends TokenAB to B.

(4) A and B perform the following steps:

Each of them verifies the received token by checking the signature contained in the token and by checking that the random number, which it previously sent to the other entity, agrees with the random number contained in the signed data of the token received.

NOTE 2 — An alternative to mechanism 5.2.3 is to run mechanism 5.1.2 both ways. The inclusion of the certificates in the first messages of mechanism 5.2.3 allows for earlier certificate verification which may speed up the authentication process.

Annex A
(informative)
Use of text fields

The tokens specified in clause 5 of this part of ISO/IEC 9798 contain text fields. The actual use of and the relationships between the various text fields in a given pass depend on the application. Some examples are given below. If a signature scheme without message recovery is used and if the signed text field is not empty, then the verifier needs to be in possession of the text prior to verifying the signature. In this annex "signed text fields" refers to text fields in the signed data and "unsigned text fields" refers to text fields in the unsigned data.

For example, if a digital signature scheme without message recovery is used, any information requiring data origin authentication should be placed in the signed text field and (as part of) the unsigned text field in the token.

If the tokens do not contain (sufficient) redundancy, the signed text fields may be used to provide additional redundancy.

Text fields may contain additional time variant parameters. For instance, a time stamp may be included in the text field(s) of TokenAB in mechanism 5.1.1 if this is used with sequence numbers. This would allow the detection of forced delays without having previously specified a time window for the acceptance of the sequence number as part of the authentication request (see also annex C).

Signed text fields may be used to indicate that the token is only valid for the purpose of entity authentication. Should there be a concern that one entity might choose a "degenerate" value with malicious intent for the other entity to sign, the other entity may introduce a random number in the text field.

Should an algorithm be used where it may be possible to launch attacks based on the fact that a particular claimant is using the same key for all verifiers with which the claimant communicates, and if such attacks are considered to be a threat, the identity of the intended verifier should be included in the signed text field and, if necessary, in the unsigned text field.

Unsigned text fields can also be used to provide information to a verifier indicating the (unauthenticated) identity which a claimant is claiming. If means other than certificates are used for distributing public keys, such information may be required to allow a verifier to determine which public key is to be used to authenticate a claimant.

Text fields could also be used for the distribution of keys (see ISO/IEC 11770-3).

Should any of the mechanisms specified in this part of ISO/IEC 9798 be embedded in an application which allows either entity to initiate the authentication by using an additional message prior to the start of the mechanism, certain intruder attacks may become possible. Text fields may be used to state which entity requests the authentication in order to counteract such attacks which are characterised by the fact that an intruder may reuse a token obtained illicitly.

Annex B
(informative)
Certificates

In this part of ISO/IEC 9798 certificates can be used to ensure the authenticity of public keys. In this case, a certificate contains an entity's distinguishing identifier, the entity's public key, and possibly other information (such as a validity period for the certificate and/or a serial number). The certificate consists of this collection of data, together with the signature of a trusted third party on this data.

The verification of a certificate consists of verifying the signature of the trusted third party, and checking, if required, other conditions related to the validity of the certificate such as the revocation or the validity period.

Certificates are not the only way of guaranteeing the authenticity of public keys. To allow an entity to obtain the public keys of other entities by other means, the use of certificates is optional in all mechanisms in this part of ISO/IEC 9798.

Annex C
(informative)
Time variant parameters

Time variant parameters are used to control uniqueness/timeliness. They enable the replay of previously transmitted messages to be detected. To achieve this, the authentication information should vary from one use of the mechanism to the next. The verifier should have either direct or indirect control over this variation.

Some types of time variant parameters may also allow the detection of "forced delays" (delays introduced into the communication medium by an adversary). In mechanisms involving more than one pass, forced delays may also be detected by other means (such as "timeout clocks" used to enforce maximum allowable time gaps between specific messages).

The three types of time variant parameters used in this part of ISO/IEC 9798 are time stamps, sequence numbers and random numbers. Implementation requirements may make different time variant parameters preferable in different applications. In some cases, it may be appropriate to use more than one time variant parameter (e.g., both time stamps and sequence numbers). Details regarding the choice of these parameters are beyond the scope of this part of ISO/IEC 9798.

C.1 Time stamps

Mechanisms involving time stamps make use of a common time reference which logically links a claimant and a verifier. The recommended reference clock is Coordinated Universal Time (UTC). An acceptance window of some fixed size is used by the verifier. Timeliness is controlled by the verifier computing the difference between the time stamp in a verified received token and the time as perceived by the verifier when the token is received. If the difference is within the window, the message is accepted. Uniqueness can be verified by logging all messages within the current window, and rejecting the second and subsequent occurrences of identical messages within that window.

Some mechanism should be used to ensure that the time clocks of the claimant and verifier are synchronised, in order that the time reference be under the verifier's (indirect) control. Moreover, time clocks need to be synchronised well enough to make the possibility of impersonation by replay acceptably small. It should also be ensured that all information relevant to the verification of time stamps, in particular the time clocks of the communicating entities, are protected against tampering.

Time stamps allow the detection of forced delays.

C.2 Sequence numbers

Uniqueness can be controlled by using sequence numbers as they enable a verifier to detect the replay of messages. A claimant and verifier agree beforehand on a policy for numbering messages in a particular manner, the general idea being that a message with a particular number will be accepted only once (or only once within a specified time period). Messages received by a verifier are then checked to see that the number sent with the message is acceptable according to the agreed policy. In this way, the sequence number is under the verifier's (indirect) control. A message is rejected if the accompanying sequence number is not in accordance with the agreed policy.

Use of sequence numbers may require additional "book-keeping". A claimant should maintain records of sequence numbers which have been used previously and/or sequence numbers which remain valid for future use. The claimant should keep such records for all potential verifiers with whom the claimant may wish to communicate. Similarly, the verifier should maintain such records corresponding to all potential claimants. Special procedures may also be required to reset and/or restart sequence number counters when situations (such as system failures) arise which disrupt normal sequencing.

Use of seqence numbers by a claimant does not guarantee that a verifier will be able to detect forced delays.

C.3 Random numbers

The random numbers used in mechanisms specified in this part of ISO/IEC 9798 prevent replay or interleaving attacks, or preclude the signing of pre-defined data. In the context of this part of ISO/IEC 9798, the use of the term random numbers also includes unpredictable pseudo-random numbers.

In order to prevent replay or interleaving attacks, the verifier obtains a random number which is sent to the claimant, and the claimant responds by including the