INTERNATIONAL STANDARD

ISO/IEC 9798-3

Second edition
1998-10-15

Information technology — Security techniques — Entity authentication —

Part 3:
Mechanisms using digital signature techniques

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

Partie 3: Mécanismes utilisant des techniques de signature numériques

Reference number
ISO/IEC 9798-3:1998(E)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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 SC27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9798-3:1993), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-3 (1st edition) will be compliant with ISO/IEC 9798-3 (2nd edition).

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

- *Part 1: General*
- *Part 2: Mechanisms using symmetric encipherment algorithms*
- *Part 3: Mechanisms using digital signature techniques*
- *Part 4: Mechanisms using a cryptographic check function*
- *Part 5: Mechanisms using zero knowledge techniques*

Further parts may follow.

Annex A of this part of ISO/IEC 9798 is for information only.

© ISO/IEC 1998

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

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

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Information technology — Security techniques — Entity authentication — Part 3:

Mechanisms using digital signature techniques

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using digital signatures based on asymmetric techniques. 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: 1997, *Information technology — Security techniques — Entity authentication — Part 1: General.*

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 identity by demonstrating its knowledge of its private signature key. This is achieved by the entity using its private 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:

a) A verifier shall possess the valid public key of the claimant, i.e., of the entity that the claimant claims to be.

b) A claimant shall have a private signature key known and used only by the claimant.

If either of these is not satisfied then the authentication process may be compromised or it cannot be completed successfully.

NOTES

1 One way of obtaining a valid public key is by means of a certificate (see Annex C of ISO/IEC 9798-1). 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.

2 References to digital signature schemes are contained in Annex D of ISO/IEC 9798-1.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5 Mechanisms

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 and Note 1 below).

Throughout this part of ISO/IEC 9798, tokens have the following form:

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

In this part of ISO/IEC 9798, the term "signed data" refers to "$Y_1||\cdots||Y_j$" used as input to the signature scheme and the term "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 contained in the text field of the signed data of the token cannot be recovered from the signature, then it shall be contained in the unsigned text field of the token.

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.

NOTES

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

2 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 B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 1.

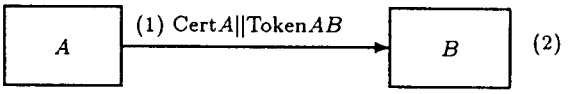

Figure 1

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

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

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 of ISO/IEC 9798-1).

(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 verifying the signature of A contained in the token, by checking the time stamp or the sequence number, 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 B of ISO/IEC 9798-1).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The authentication mechanism is illustrated in figure 2.

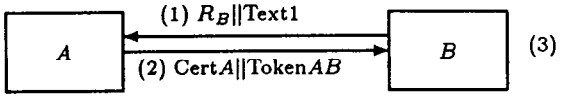

Figure 2

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 identifier B in TokenAB is optional. It depends on the environment in which this authentication mechanism is used.

NOTES

1 The inclusion of the optional identifier B in the signed data of TokenAB can prevent the token from being accepted by anyone other than the intended verifier (e.g., in a person-in-the-middle attack).

2 The inclusion of the random number R_A in the signed part of TokenAB prevents B from obtaining the 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 key is used by A for purposes other than 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, 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, and by checking that the value of the identifier field (B) in the signed data of TokenAB, if present, is equal to B's distinguishing identifier.

5.2 Mutual authentication

Mutual authentication means that the two communicating entities are authenticated to each other.

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 B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 3.

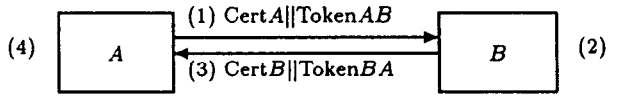

Figure 3

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

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

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

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

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. Further binding together of these messages can be achieved by making appropriate use of the text fields.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.2.2 Three pass authentication

In this authentication mechanism uniqueness / timeliness is controlled by generating and checking random numbers (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 4.

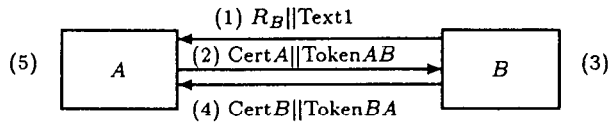

Figure 4

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 inclusion of the random number R_A in the signed part of TokenAB prevents B from obtaining the 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 key is used by A for purposes other than entity authentication. However, the inclusion of R_B in TokenBA, whilst necessary for security reasons which dictate that A should check that it is the same as the value sent in the first message, may not offer the same protection to B, since R_B is known to A before R_A is chosen. If this type of protection is required, B can insert an additional random number R'_B in the text fields Text4 and Text5 of TokenBA.

(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, 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, and by checking that the value of the identifier field (B) in the signed data of TokenAB, if present, is equal to B's distinguishing identifier.

(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 B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 5.

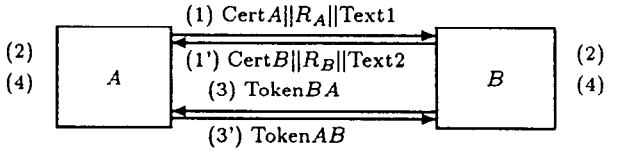

Figure 5

The tokens are similar to those of clause 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. Depending on the relative time of receipt of the messages sent in steps (1) and (1'), one of the parties may know the random number of the other party when choosing its random number. If this is undesirable, both parties can insert an additional random number R'_A and R'_B in the text fields Text3 and Text4 of TokenAB, and Text5 and Text 6 of TokenBA, respectively.

(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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

(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) A sends TokenAB to B.

(3') B sends TokenBA to A.

(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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC

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; see also Annex A of ISO/IEC 9798-1.

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.

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC

ICS 35.040

Descriptors: data processing, information interchange, data transmission, protection of information, security techniques, coding (data conversion), authentication, message authentication codes, algorithms.

Price based on 6 pages

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale