INTERNATIONAL STANDARD

ISO/IEC 9798-1

Second edition
1997-08-01

Information technology — Security techniques — Entity authentication —

Part 1:
General

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

Partie 1: Généralités

Reference number
ISO/IEC 9798-1:1997(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 9798–1 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 9798-1:1991), which has been technically revised.

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

- *Part 3: Entity authentication using a public key algorithm*

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 4: Mechanisms using a cryptographic check function*
- *Part 5: Mechanisms using asymmetric zero knowledge techniques*

> NOTE — The introductory element of the title of part 3 will be aligned with the introductory element of the titles of parts 1, 2, 4 and 5 at the next revision of part 3 of ISO/IEC 9798.

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 —

Part 1:
General

1 Scope

This part of ISO/IEC 9798 specifies an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities, and where required, exchanges with a trusted third party.

The details of the mechanisms and the contents of the authentication exchanges are not specified in this part of ISO/IEC 9798 but in the subsequent parts.

Certain of the mechanisms specified in subsequent parts of ISO/IEC 9798 can be used to help provide non-repudiation services, mechanisms for which are specified in ISO/IEC 13888. The provision of non-repudiation services is beyond the scope of ISO/IEC 9798.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the editions indicated were 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 editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2: 1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture.*

ISO/IEC 9594-8: 1995, *Information technology — Open Systems Interconnection — The Directory — Part 8: Authentication framework.*

ISO/IEC 10181-2: 1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework.*

ISO/IEC 13888-1 —[1]: *Information technology — Security techniques — Non-repudiation— Part 1: General.*

3 Definitions

3.1 ISO/IEC 9798 makes use of the following general security-related terms defined in ISO 7498-2:

3.1.1 cryptographic check value: information which is derived by performing a cryptographic transformation on the data unit.

3.1.2 masquerade: the pretence by an entity to be a different entity.

3.1.3 digital signature (signature): data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

3.2 ISO/IEC 9798 makes use of the following general security-related terms defined in ISO/IEC 10181-2:

3.2.1 claimant: an entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

3.2.2 principal: an entity whose identity can be authenticated.

[1] to be published

3.2.3 trusted third party: a security authority or its agent, trusted by other entities with respect to security-related activities. In the context of ISO/IEC 9798, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

3.2.4 verifier: an entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

3.3 For the purposes of ISO/IEC 9798 the following definitions apply:

3.3.1 asymmetric cryptographic technique: a cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

NOTE — A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature systems, encipher and decipher for encipherment systems. The signature and decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, since this is not the general case, throughout ISO/IEC 9798 the four elementary transformations and the corresponding keys are kept separate.

3.3.2 asymmetric encipherment system: a system based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment.

3.3.3 asymmetric key pair: a pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

3.3.4 asymmetric signature system: a system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification.

3.3.5 challenge: a data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier.

3.3.6 ciphertext: data which has been transformed to hide its information content.

3.3.7 cryptographic check function: a cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall be infeasible.

3.3.8 decipherment: the reversal of a corresponding encipherment.

3.3.9 distinguishing identifier: information which unambiguously distinguishes an entity.

3.3.10 encipherment: the (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data.

3.3.11 entity authentication: the corroboration that an entity is the one claimed.

3.3.12 interleaving attack: a masquerade which involves use of information derived from one or more ongoing or previous authentication exchanges.

3.3.13 key: a sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

3.3.14 mutual authentication: entity authentication which provides both entities with assurance of each other's identity.

3.3.15 plaintext: unenciphered information.

3.3.16 private decipherment key: private key which defines the private decipherment transformation.

3.3.17 private key: that key of an entity's asymmetric key pair which should only be used by that entity.

NOTE — In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation.

3.3.18 private signature key: private key which defines the private signature transformation.

NOTE — This is sometimes referred to as a secret signature key.

3.3.19 public encipherment key: public key which defines the public encipherment transformation.

3.3.20 public key: that key of an entity's asymmetric key pair which can be made public.

NOTE — In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a prespecified group.

3.3.21 public key certificate (certificate): the public key information of an entity signed by the certification authority and thereby rendered unforgeable (see also Annex C).

3.3.22 public key information: information specific to a single entity and which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, and the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms (see also Annex C).

3.3.23 public verification key: public key which defines the public verification transformation.

3.3.24 random number: a time variant parameter whose value is unpredictable (see also Annex B).

3.3.25 reflection attack: a masquerade which involves sending a previously transmitted message back to its originator.

3.3.26 replay attack: a masquerade which involves use of previously transmitted messages.

3.3.27 sequence number: a time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period (see also Annex B).

3.3.28 symmetric cryptographic technique: a cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

3.3.29 symmetric encipherment algorithm: an encipherment algorithm that uses the same secret key for both the originator's and the recipient's transformation.

3.3.30 time stamp: a time variant parameter which denotes a point in time with respect to a common reference (see also Annex B).

3.3.31 time variant parameter: a data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp (see also Annex B).

3.3.32 token: a message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique.

3.3.33 unilateral authentication: entity authentication which provides one entity with assurance of the other's identity but not vice versa.

4 Notation

Throughout ISO/IEC 9798 the following notation is used:

A: the distinguishing identifier of entity A.

B: the distinguishing identifier of entity B.

TP: the distinguishing identifier of the trusted third party.

K_{XY}: a secret key shared between entities X and Y, used only in symmetric cryptographic techniques.

P_X: a public verification key associated with entity X, used only in asymmetric cryptographic techniques.

S_X: a private signature key associated with entity X, used only in asymmetric cryptographic techniques.

N_X: a sequence number issued by entity X.

R_X: a random number issued by entity X.

T_X: a time stamp issued by entity X.

$\frac{T_X}{N_X}$: a time variant parameter originated by entity X which is either a time stamp T_X or a sequence number N_X .

$Y||Z$: the result of the concatenation of the data items Y and Z in that order.

$eK(Z)$: the result of the encipherment of data Z with a symmetric encipherment algorithm using the key K.

$dK(Z)$: the result of the decipherment of data Z with a symmetric encipherment algorithm using the key K.

$f_K(Z)$: a cryptographic check value which is the result of applying the cryptographic check function f using as input a secret key K and an arbitrary data string Z.

CertX: a trusted third party's certificate for entity X.

TokenXY: a token sent from entity X to entity Y.

TVP: a time variant parameter.

$sS_X(Z)$: the signature resulting from applying the private signature transformation on data Z using the private signature key S_X.

5 Authentication model

The general model for entity authentication mechanisms is shown in Figure 1. It is not essential that all the entities and exchanges are present in every authentication mechanism.

For the authentication mechanisms specified in the other parts of ISO/IEC 9798, for unilateral authentication, entity A is considered the claimant, and entity B is considered the verifier. For mutual authentication, A and B each take the roles of both claimant and verifier.

For authentication purposes, the entities generate and exchange standardised messages, called tokens. It takes the exchange of at least one token for unilateral authentication and the exchange of at least two tokens for mutual authentication. An additional pass may be needed if a challenge has to be sent to initiate the authentication exchange. Additional passes may be needed if a trusted third party is involved.

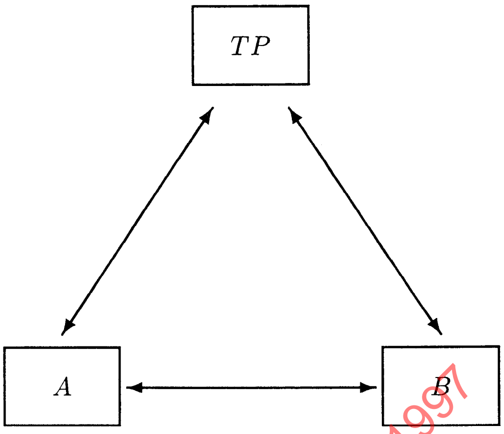

Figure 1 – Authentication model

In Figure 1, the lines indicate potential information flow. Entities A and B may either directly interact with each other, directly interact with the trusted third party TP, indirectly interact with the trusted third party through B or A respectively, or use some information issued by the trusted third party.

The details of the authentication mechanisms of ISO/IEC 9798 are specified in the subsequent parts.

6 General requirements and constraints

In order that an entity can authenticate another entity, both shall use a common set of cryptographic techniques and parameters.

During the operational life of a key, the values of all time-variant parameters on which the key operates (i.e., time stamps, sequence numbers, and random numbers) shall be non-repeating, at least with overwhelming probability.

It is assumed that, during use of an authentication mechanism, the entities A and B are aware of each other's claimed identities. This may be achieved by the inclusion of identifiers in information exchanged between the two entities, or it may be apparent from the context of the use of the mechanism.

The authenticity of the entity can be ascertained only for the instant of the authentication exchange. To guarantee the authenticity of subsequent communicated data, the authentication exchange must be used in conjunction with a secure means of communication (e.g., an integrity service).

Annex A
(informative)

Use of text fields

The tokens specified in the following parts 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.

Text fields may contain additional time variant parameters. For instance, a time stamp may be included in the text field(s) of a token if this is used with sequence numbers. This would allow the detection of forced delays by requiring the recipient of a message to verify that any time stamp contained in the message is within a prespecified time window (see also Annex B).

If more than one valid key exists, then an identifier of the key may be included in a text field in the plaintext. If more than one trusted third party exists, then text fields could be used to include the distinguishing identifier of the trusted third party in question.

Text fields could also be used for the distribution of keys (see ISO/IEC 11770–2 and ISO/IEC 11770–3).

Should any of the mechanisms specified in the following parts 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 characterized by the fact that an intruder may reuse a token obtained illicitly (see ISO/IEC 10181-2).

The above examples are not exhaustive.

Annex B
(informative)
Time variant parameters

Time variant parameters are used to control uniqueness/timeliness. They enable replay of previously transmitted messages to be detected. To achieve this, the authentication information should vary from one exchange instance to the next.

Some types of time variant parameters may also allow for 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 the following parts 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 type of 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.

B.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 at the time 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 communicating entities are synchronised. Moreover, time clocks need to be synchronized 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 two communicating entities, are protected against tampering.

Mechanisms using time stamps allow the detection of forced delays.

B.2 Sequence numbers

Uniqueness can be controlled 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 along with the message is acceptable according to the agreed policy. A message is rejected if the accompanying sequence number is not in accordance with the agreed policy.

Use of sequence numbers may require additional "bookkeeping". A claimant should maintain records of sequence numbers which have been used previously and/or sequence numbers that 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 sequence numbers by a claimant does not guarantee that a verifier will be able to detect forced delays. For mechanisms involving two or more messages, forced delays can be detected if the sender of a message measures the time interval between transmission of a message and receipt of an expected reply, and rejects it if the delay is more than a prespecified time slot.

B.3 Random numbers

The random numbers as used in mechanisms specified in the following parts of ISO/IEC 9798 prevent replay or interleaving attacks. It is therefore required that all random numbers used in ISO/IEC 9798 are chosen from a sufficiently large range so that the probability of repetition is very small when used with the same key, and also that the probability of a third party predicting a specific value is very small. In the context of ISO/IEC 9798, the use of the term random numbers also includes pseudorandom numbers satisfying the same requirements.

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 random number in the protected part of the returned token. (This is commonly referred to as challenge-response.) This procedure links the two messages containing the particular random number. If the same random number were to be used by the verifier again, a third party that recorded the original authentication exchange could send the recorded token to the verifier and falsely authenticate itself as the claimant. The requirement that the random number be non-repeating with very high probability is present in order to prevent such attacks.

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