INTERNATIONAL STANDARD

ISO/IEC 9798-4

First edition
1995-03-15

Information technology — Security techniques — Entity authentication —

Part 4:
Mechanisms using a cryptographic check function

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

Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

Reference number
ISO/IEC 9798-4:1995(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 9798–4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-Committee SC27, *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 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 2: Mechanisms using symmetric encipherment algorithms
- Part 4: Mechanisms using a cryptographic check function
- Part 5: Mechanisms using zero knowledge techniques

NOTE — The introductory element of the titles of parts 1 and 3 will be aligned with the introductory element of the titles of parts 2,4 and 5 at the next revision of parts 1 and 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.

Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using a cryptographic check function. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities.

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 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 passes are required to achieve mutual authentication.

Examples of cryptographic check functions are given in annex C.

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. In addition the following definition and notation are used:

3.1 cryptographic check value: Information which is derived by performing a cryptographic transformation on the data unit [ISO 7498-2].

3.2 $f_K(Z)$**:** 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.

3.3 $\begin{matrix} T_A \\ N_A \end{matrix}$**:** Time variant parameter originated by entity A which is either a time stamp T_A or a sequence number N_A .

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 a secret authentication key. This is achieved by the entity using its secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. The cryptographic check value can be checked by anyone knowing the entity's secret authentication key who can re-calculate the cryptographic check value and compare it with the value received.

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

a) A claimant authenticating itself to a verifier shares a common secret authentication key with that verifier. This key shall be known to the involved entities prior

to the commencement of any particular run of an authentication mechanism. The method by which the key is distributed to the entities is beyond the scope of this part of ISO/IEC 9798.

b) The secret authentication key, shared by a claimant and a verifier, shall be known only to those two entities and, possibly, to other parties they both trust.

c) The cryptographic check function f which takes as input a secret key K and an arbitrary string Z to produce $f_K(Z)$ shall satisfy the following properties:

- for any key K and data string Z it shall be practical to compute $f_K(Z)$;
- for any fixed key K, and given no prior knowledge of K, it shall be computationally infeasible to find a new pair (X, Y) such that $f_K(X) = Y$, even given knowledge of a set of pairs (X_i, Y_i) such that $f_K(X_i) = Y_i$, $(i = 1, 2, \ldots)$, where the value of X_i may have been chosen after observing the value of Y_j $(j = 1, 2, \ldots, i-1)$.

d) The strength of the mechanisms is dependent on the length and the secrecy of the key, on the nature of the cryptographic check function, and on the length of the check value. These parameters shall be chosen to meet the required security level, as may be specified by the security policy.

5 Mechanisms

In these authentication mechanisms the entities A and B shall share a common secret authentication key K_{AB} or two uni-directional secret keys K_{AB} and K_{BA} prior to the commencement of any particular run of the authentication mechanisms. In the latter case the uni-directional keys K_{AB} and K_{BA} are used respectively for the authentication of A by B and of B by A.

The mechanisms require the use of time variant parameters such as time stamps, sequence numbers or random numbers. The properties of these parameters, in particular that it is most unlikely for them to repeat within the life-time of an authentication key, are important for the security of these mechanisms. For additional information see annex B.

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 relation and contents further depend upon the specific application. See annex A for information on the use of text fields.

A text field may only be included in the input to the cryptographic check function if the verifier can determine it independently, e.g., if it is known in advance, sent in clear or can be derived from one or both of those sources.

Unilateral authentication 5.1 U

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

One pass authentication 5.1.1 I

n 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).

The authentication mechanism is illustrated in figure 1.

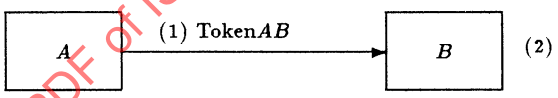

Figure 1

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

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

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.

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE — Distinguishing identifier B is included in TokenAB to prevent the re-use of TokenAB on entity A by an adversary masquerading as entity B. Its inclusion is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if a uni-directional key is used.

(1) A sends TokenAB to B.

(2) On receipt of the message containing TokenAB, B verifies TokenAB by checking the time stamp or the sequence number, calculating

$$f_{K_{AB}}\left({}^{T_A}_{N_A}\|B\|\text{Text1}\right)$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, as well as the time stamp or the sequence number.

Two pass authentication 5.1.2 I

n 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).

The authentication mechanism is illustrated in figure 2.

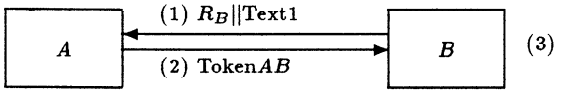

Figure 2

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

$$\text{Token}AB = \text{Text3} || f_{K_{AB}}(R_B || B || \text{Text2}).$$

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE — Distinguishing identifier B is included in TokenAB to prevent a so-called reflection attack. Such an attack is characterized by the fact that an intruder "reflects" the challenge R_B to B pretending to be A. The inclusion of the distinguishing identifier B is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if a uni-directional key is used.

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

(2) A sends TokenAB to B.

(3) On receipt of the message containing TokenAB, B verifies TokenAB by calculating

$$f_{K_{AB}}(R_B || B || \text{Text2})$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, and that the random number R_B, sent to A in step (1), was used in constructing TokenAB.

Mutual authentication 5.2 M

utual 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 adapted in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. In both cases this requires one more pass resulting in two more steps.

NOTE — A third mechanism for mutual authentication can be constructed from two instances of the mechanism specified in 5.1.2, one started by entity A and the other by entity B.

Two pass authentication 5.2.1 I

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

The authentication mechanism is illustrated in figure 3.

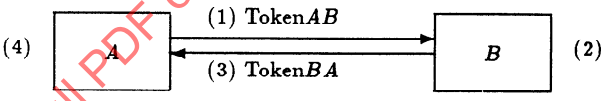

Figure 3

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

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

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

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

The inclusion of the distinguishing identifier B in TokenAB and the inclusion of the distinguishing identifier A in TokenBA are (independently) optional.

NOTE 1 — Distinguishing identifier B is included in TokenAB to prevent the re-use of TokenAB on entity A by an adversary masquerading as entity B. For similar reasons the distinguishing identifier A is present in TokenBA. Their inclusion is made optional so that, in environments where such attacks cannot occur, one or both may be omitted.

The distinguishing identifiers A and B may also be omitted if uni-directional keys (see below) are used.

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

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

(3) B sends TokenBA 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 (see annex A).

If uni-directional keys are used then the key K_{AB} in TokenBA is replaced by the uni-directional key K_{BA} and the appropriate key is used in step (4).

Three pass authentication 5.2.2 I

n this mutual authentication mechanism uniqueness / timeliness is controlled by generating and checking random numbers (see annex B).

The authentication mechanism is illustrated in figure 4.

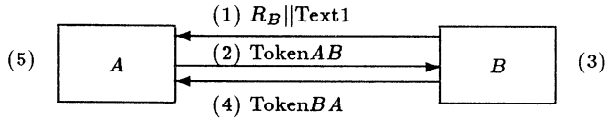

Figure 4

The tokens are of the following form:

TokenAB = R_A||Text3||$f_{K_{AB}}$ (R_A||R_B||B||Text2).
TokenBA = Text5||$f_{K_{AB}}$ (R_B||R_A||Text4).

NOTE 1 — The inclusion of R_B in TokenBA prevents the derivation of TokenBA from TokenAB.

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE 2 — Distinguishing identifier B is included in TokenAB to prevent a so-called reflection attack. Such an attack is characterized by the fact that an intruder "reflects" the challenge R_B to B pretending to be A. The inclusion of the distinguishing identifier B is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if uni-directional keys (see below) are used.

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

(2) A sends TokenAB to B.

(3) On receipt of the message containing TokenAB, B verifies TokenAB by calculating

$$f_{K_{AB}}\,(R_A||R_B||B||\text{Text2})$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, and that the random number R_B, sent to A in step (1), was used in constructing TokenAB.

(4) B sends TokenBA to A.

(5) On receipt of the message containing TokenBA, A verifies TokenBA by calculating

$$f_{K_{AB}}\,(R_B||R_A||\text{Text4})$$

and comparing it with the cryptographic check value of the token, thereby verifying that the random number R_B, received from B in step (1) was used in constructing in TokenBA and that the random number R_A, sent to B in step (2), was used in constructing TokenBA.

If uni-directional keys are used then the key K_{AB} in TokenBA is replaced by the uni-directional key K_{BA} and the appropriate key is used in step (5).

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.

Any information requiring data origin authentication should be used in the calculation of the cryptographic check value of the token.

Text fields may contain additional time variant parameters. For instance, if mechanism 5.1.1 is used with sequence numbers, then a time stamp may be included in the text fields of TokenAB. 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 the cleartext text field may include the key identifier.

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 characterized by the fact that an intruder may reuse a token obtained illicitly.

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. The verifier should have either direct or indirect control over this variation.

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 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 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 claimant and verifier are synchronised, in order that the time reference be under the verifier's (indirect) control. 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. 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 "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 this part of ISO/IEC 9798 prevent replay or interleaving attacks. 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 random number in the authentication data 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 is used by the verifier again, a third party that recorded the original authentication exchange can send the recorded token to the verifier and falsely authenticate itself as the claimant. In order to prevent such attacks, it is necessary for the random numbers to be non-repeating with a very high probability.

Random numbers are by definition unpredictable, and can be considered non-repeating with a high degree of probability if they take values from a sufficiently large range.

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