INTERNATIONAL STANDARD

# ISO/IEC 9798-4

Second edition
1999-12-15



# Information technology — Security techniques — Entity authentication —

## Part 4: Mechanisms using a cryptographic check function

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

*Partie 4: Mécanismes utilisant une fonction cryptographique de vérification*

Reference number
ISO/IEC 9798-4:1999(E)

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.





ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

## Contents

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

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.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 9798 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 9798-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques.*

This second edition cancels and replaces the first edition (ISO/IEC 9798-4:1995), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-4 (1st edition) will be compliant with ISO/IEC 9798-4 (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.

# 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 or more than once.

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 ISO/IEC 9797.

## 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, 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 normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs).*

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 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 sharing 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 parties 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 strength of the mechanisms is dependent on the length and the secrecy of the key, on the nature of the cryptographic check functions, 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 unidirectional secret keys $K_{AB}$ and $K_{BA}$ prior to the commencement of any particular run of the authentication mechanisms. In the latter case, the unidirectional 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 the time variant parameters are important for the security of these mechanisms. In particular, the parameters shall be chosen so that it shall be most unlikely for them to repeat within the lifetime of an authentication key. For additional information see annex B of ISO/IEC 9798-1.

The use of the text fields specified in the following mechanisms is outside the scope of this part of ISO/IEC 9798 (they may be empty), and will 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.

### 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 (Token$AB$), sent by the claimant $A$ to the verifier $B$ is:

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

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. As defined in ISO/IEC 9798-1, $f_K(X)$ denotes the cryptographic check value computed by applying the cryptographic check function $f$ to the data $X$ using the key $K$.

The inclusion of the distinguishing identifier $B$ in Token$AB$ is optional.

NOTE Distinguishing identifier $B$ is included in Token$AB$ to prevent the re-use of Token$AB$ 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 unidirectional key is used.

(1) $A$ generates and sends Token$AB$ to $B$.

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

$$f_{K_{AB}}(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| \text{Text1})$$

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.

### 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).

The authentication mechanism is illustrated in figure 2.

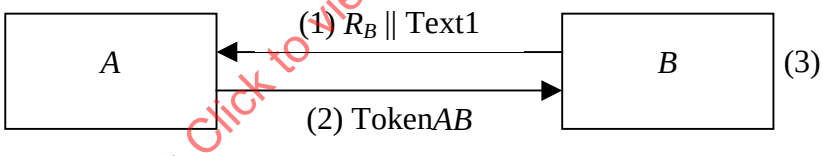


**Figure 2**

The form of the token (Token$AB$), 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 Token$AB$ is optional.

NOTE Distinguishing identifier $B$ is included in Token$AB$ to prevent a so-called reflection attack. Such an attack is characterised 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 unidirectional key is used.

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

(2) $A$ generates and sends Token$AB$ to $B$.

(3) On receipt of the message containing Token$AB$, $B$ verifies Token$AB$ by calculating

$$f_{K_{AB}}(R_B \,||\, B \,||\, \text{Text}2)$$

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 Token$AB$.

## 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 adapted in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. In both cases this requires one more pass and results 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 $B$.

### 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.

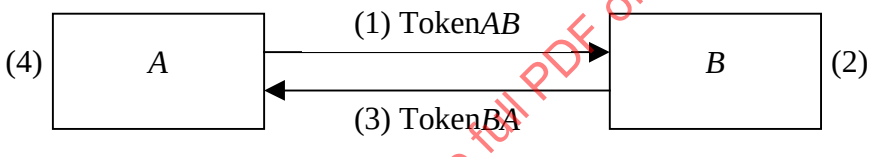


**Figure 3**

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

$$\text{Token}AB = \begin{matrix} T_A \\ N_A \end{matrix} \,||\, \text{Text}2 \,||\, f_{K_{AB}}\left(\begin{matrix} T_A \\ N_A \end{matrix} \,||\, B \,||\, \text{Text}1\right).$$

The form of the token (Token$BA$), sent by $B$ to $A$, is:

$$\text{Token}BA = \begin{matrix} T_B \\ N_B \end{matrix} \,||\, \text{Text}4 \,||\, f_{K_{AB}}\left(\begin{matrix} T_B \\ N_B \end{matrix} \,||\, A \,||\, \text{Text}3\right).$$

The inclusion of the distinguishing identifier $B$ in Token$AB$ and the inclusion of the distinguishing identifier $A$ in Token$BA$ are (independently) optional.

NOTE 1 Distinguishing identifier $B$ is included in Token$AB$ to prevent the re-use of Token$AB$ on entity $A$ by an adversary masquerading as entity $B$. For similar reasons the distinguishing identifier $A$ is present in Token$BA$. 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 unidirectional 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) $B$ generates and sends Token$BA$ 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 unidirectional keys are used then the key $K_{AB}$ in Token$BA$ is replaced by the unidirectional key $K_{BA}$ and the appropriate key is used in step (4).

### 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.

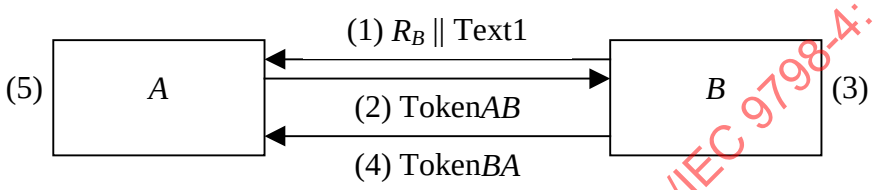


**Figure 4**

The tokens are of the following form:

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

$$\text{Token}BA = \text{Text5} \,||\, f_{K_{AB}}(R_B \,||\, R_A \,||\, \text{Text4}).$$

The inclusion of the distinguishing identifier $B$ in Token$AB$ is optional.

NOTE When present, distinguishing identifier $B$ is included in Token$AB$ to prevent a so-called reflection attack. Such an attack is characterised 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 unidirectional keys (see below) are used.

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

(2) $A$ generates a random number $R_A$, and generates and sends Token$AB$ to $B$.

(3) On receipt of the message containing Token$AB$, $B$ verifies Token$AB$ 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 Token$AB$.

(4) $B$ generates and sends Token$BA$ to $A$.

(5) On receipt of the message containing Token$BA$, $A$ verifies Token$BA$ by calculating

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