INTERNATIONAL STANDARD

ISO/IEC 9798-2

Third edition
2008-12-15

Information technology — Security techniques — Entity authentication —

Part 2:
Mechanisms using symmetric encipherment algorithms

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

Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

Reference number
ISO/IEC 9798-2:2008(E)

© ISO/IEC 2008

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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 International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 9798-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 9798-2:1999), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 9798-2:1999/Cor.1:2004. Note that implementations which conform to the second edition will conform to the third 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*

— *Part 6: Mechanisms using manual data transfer*

Further parts may follow.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

© ISO/IEC 2008 – All rights reserved

Information technology — Security techniques — Entity authentication —

Part 2:
Mechanisms using symmetric encipherment algorithms

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using symmetric encipherment algorithms. Four of the mechanisms provide entity authentication between two entities where no trusted third party is involved; two of these are mechanisms to unilaterally authenticate one entity to another, while the other two are mechanisms for mutual authentication of two entities. The remaining mechanisms require a trusted third party for the establishment of a common secret key, and realize mutual or unilateral entity authentication.

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 no trusted third party is involved and 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 no trusted third party is involved and 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. If a trusted third party is involved, any additional communication between an entity and the trusted third party requires two extra passes in the communication exchange.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9798-1, *Information technology — Security techniques — Entity authentication — Part 1: General*

© ISO/IEC 2008 – All rights reserved

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 9798-1 and the following apply.

3.1
authenticated encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, data integrity, and data origin authentication

[ISO/IEC 19772:—[1)]]

3.2
ciphertext
data which has been transformed to hide its information content

[ISO/IEC 10116:2006]

3.3
claimant
entity whose identity can be authenticated, including the functions and the private data necessary to engage in authentication exchanges on behalf of a principal

[ISO/IEC 9798-5:2004]

3.4
message authentication code
MAC
string of bits which is the output of a MAC algorithm

NOTE A MAC is sometimes called a cryptographic check value.

[ISO/IEC 9797-1:1999]

3.5
message authentication code (MAC) algorithm
algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties:

- for any key and any input string the function can be computed efficiently;
- for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first $i - 1$ function values.

NOTE 1 A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2).

NOTE 2 Computational feasibility depends on the user’s specific security requirements and environment.

[ISO/IEC 9797-1:1999]

3.6
time stamp
time variant parameter which denotes a point in time with respect to a common time reference

[ISO/IEC 18014-1:2008]

1) To be published.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

© ISO/IEC 2008 – All rights reserved

3.7
trusted third party
TTP
security authority, or its agent, trusted by other entities with respect to security-related activities

[ISO/IEC 18014-1:2008]

4 Symbols and notation

A, *B*	Labels used for the entities participating in a mechanism.
d_K	An authenticated decipherment process using secret key *K*.
e_K	An authenticated encipherment process performed using secret key *K*.
$e_K(X)$	A result of the encipherment process for data *X* with a symmetric encipherment algorithm using a key *K*.
I_U	A distinguishing identifier of entity *U*.
K	A secret key used with the encipherment and decipherment processes.
K_{UV}	A secret key shared between entities *U* and *V* used only in symmetric encipherment techniques.
N_U	A sequence number issued by entity *U*.
P	A symbol used to represent the trusted third party.
R_U	A random number issued by entity *U*.
TN_U	A time variant parameter originated by entity *U* which is either a time stamp T_U or a sequence number N_U.
$Token_{UV}$	A token sent from entity *U* to entity *V*.
T_U	A time stamp issued by entity *U*.
TVP_U	A time variant parameter originated by entity *U* which is a time stamp T_U, a sequence number N_U or a random number R_U.
$X \parallel Y$	The result of the concatenation of the data items *X* and *Y* in that order. (See NOTE.)
NOTE The concatenation process should incorporate any necessary encoding to ensure that there is no ambiguity in the interpretation of the concatenated string.	

5 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 to encipher specific data. The enciphered data can be deciphered by anyone sharing the entity's secret authentication key. The deciphered data must include a time variant parameter. The parameter can be verified in the following ways.

1. If it is a random number, then the recipient should make sure it is identical to the random challenge sent to the claimant. As for creation and use of random numbers, refer to ISO/IEC 18031.

2. If it is a time stamp, the recipient should verify the validity of the time stamp.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

3. If it is a sequence number, then the recipient must be able to compare it with previously received or stored sequence number(s) to make sure it is not a replay.

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 claimant authenticating itself to a verifier shall share a common secret authentication key with that verifier, in which case the mechanisms of Clause 6 apply, or each entity shall share a secret authentication key with a common trusted third party, in which case the mechanisms of Clause 7 apply. Such keys shall be known to the involved parties prior to the commencement of any particular occurrence of an authentication mechanism. The method by which this is achieved is beyond the scope of this part of ISO/IEC 9798. Guidance on the management of shared secret keys is provided in ISO/IEC 11770-1 and ISO/IEC 11770-2.

b) If a trusted third party is involved, it shall be trusted by both the claimant and the verifier.

c) The secret authentication key shared by a claimant and a verifier, or by an entity and a trusted third party, shall be known only to those two parties and, possibly, to other entities which they both trust not to misuse the key, e.g. to masquerade as one of the parties.

NOTE The encipherment algorithm and the key lifetime should be chosen so that it is computationally infeasible for a key to be deduced during its lifetime. In addition, the key lifetime should be chosen to prevent known plaintext or chosen plaintext attacks.

d) The tokens used in the mechanisms must be unforgeable even with the knowledge of old tokens. In other words, old tokens must not be reusable in any way (in part or in full) to construct new tokens. For every possible secret key K, the encipherment function e_K and its corresponding decipherment function d_K shall have the following property. The decipherment process d_K, when applied to a string $e_K(X)$, shall enable the recipient of that string to detect forged or manipulated data, i.e. only the possessor of the secret key K shall be capable of generating strings which will be 'accepted' when subjected to the decipherment process d_K.

NOTE In practice, this can be achieved in many ways. The recommended approach is to use the secret key K with an authenticated encryption technique that provides both confidentiality and integrity protection, as standardised in ISO/IEC 19772.

e) The mechanisms in this part of ISO/IEC 9798 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 lifetime of a secret authentication key, are important for the security of these mechanisms. For additional information see Annex B of ISO/IEC 9798-1:1997.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

6 Mechanisms not involving a trusted third party

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 occurrence 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.

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 B for information on the use of text fields.

6.1 Unilateral authentication

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

6.1.1 Mechanism 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 9798-1:1997). The authentication mechanism is illustrated in Figure 1.

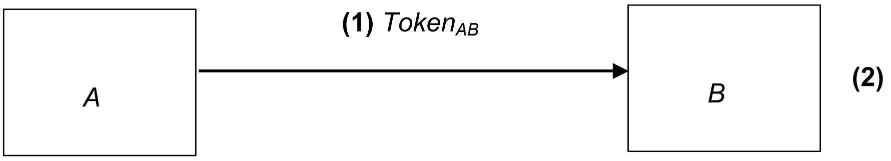

Figure 1 — Mechanism 1 — One-pass authentication

The form of the token ($Token_{AB}$), sent by the claimant *A* to the verifier *B* is:

$$Token_{AB} = Text_2 \,||\, e_{K_{AB}}(\, TN_A \,||\, I_B \,||\, Text_1 \,)$$

where the claimant *A* uses a time variant parameter TN_A which is a time stamp T_A or a sequence number N_A. 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 I_B in $Token_{AB}$ is optional.

NOTE Distinguishing identifier I_B is included in $Token_{AB}$ to prevent the reuse 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 I_B may also be omitted if a unidirectional key is used.

The following is a description of Mechanism 1 — One-pass authentication:

(1) *A* generates and sends $Token_{AB}$ to *B*.

(2) On receipt of the message containing $Token_{AB}$, *B* verifies $Token_{AB}$ by deciphering the enciphered part [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifier I_B, if present, as well as the time stamp or the sequence number.

6.1.2 Mechanism 2 — Two-pass authentication

In this authentication mechanism the claimant *A* is authenticated by the verifier *B* that initiates the process. Uniqueness/timeliness is controlled by generating and checking a random number R_B (see Annex B of ISO/IEC 9798-1:1997). The authentication mechanism is illustrated in Figure 2.

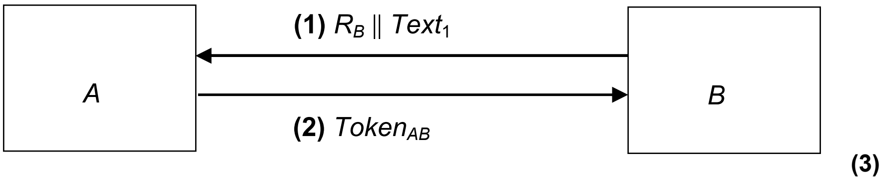

Figure 2 — Mechanism 2 — Two-pass authentication

The form of the token ($Token_{AB}$), sent by the claimant *A* to the verifier *B* is:

$$Token_{AB} = Text_3 \,||\, e_{K_{AB}}(\, R_B \,||\, I_B \,||\, Text_2 \,)$$

The inclusion of the distinguishing identifier I_B in $Token_{AB}$ is optional.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

NOTE 1 In order to prevent the possibility of a chosen plaintext attack, i.e. a cryptanalytic attack where the cryptanalyst knows the complete plaintext for one or more ciphertext strings, entity A may include a random number R_A in $Text_2$.

NOTE 2 Distinguishing identifier I_B is included in $Token_{AB}$ to prevent any party from using $Token_{AB}$ as $Token_{BA}$. The inclusion of the distinguishing identifier I_B is made optional so that, in environments where such attacks cannot occur, it may be omitted. The distinguishing identifier I_B may also be omitted if a unidirectional key is used.

The following is a description of Mechanism 2 — Two-pass authentication:

(1) *B* generates a random number R_B and sends it and, optionally, a text field $Text_1$ 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 deciphering the enciphered part [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifier I_B, if present, and that the random number R_B, sent to *A* in step (1), agrees with the random number contained in $Token_{AB}$.

6.2 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 6.1.1 and 6.1.2 are adapted in 6.2.1 and 6.2.2, 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 6.1.2, one started by entity *A* and the other by entity *B*.

6.2.1 Mechanism 3 — 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 9798-1:1997).

The authentication mechanism is illustrated in Figure 3.

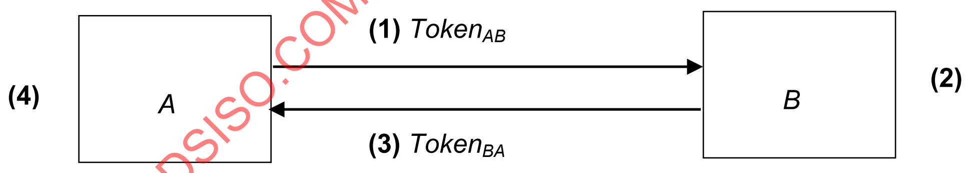

Figure 3 — Mechanism 3 — Two-pass authentication

The form of the token ($Token_{AB}$), sent by *A* to *B*, is identical to that specified in 6.1.1.

$$Token_{AB} = Text_2 \,\|\, e_{K_{AB}} \left(TN_A \,\|\, I_B \,\|\, Text_1 \right)$$

The form of the token ($Token_{BA}$), sent by *B* to *A*, is:

$$Token_{BA} = Text_4 \,\|\, e_{K_{AB}} \left(TN_B \,\|\, I_A \,\|\, Text_3 \right)$$

The inclusion of the distinguishing identifier I_B in $Token_{AB}$ and the inclusion of the distinguishing identifier I_A in $Token_{BA}$ are (independently) optional.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

© ISO/IEC 2008 – All rights reserved

NOTE Distinguishing identifier I_B is included in $Token_{AB}$ to prevent the reuse of $Token_{AB}$ on entity A by an adversary masquerading as entity B. For similar reasons the distinguishing identifier I_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 I_A and I_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.

The following is a description of Mechanism 3 — Two-pass authentication:

(1) A generates and sends $Token_{AB}$ to B.

(2) On receipt of the message containing $Token_{AB}$, B verifies $Token_{AB}$ by deciphering the enciphered part [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifier I_B, if present, as well as the time stamp or the sequence number.

(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 6.1.1.

NOTE 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 6.1.1 twice. Further binding together of these messages can be achieved by making appropriate use of text fields.

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).

6.2.2 Mechanism 4 — Three-pass authentication

In this authentication mechanism uniqueness/timeliness is controlled by generating and checking random numbers (see Annex B of ISO/IEC 9798-1:1997).

The authentication mechanism is illustrated in Figure 4.

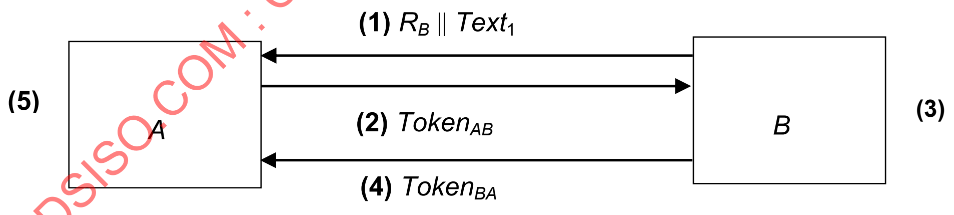

Figure 4 — Mechanism 4 — Three-pass authentication

The tokens are of the following form:

$$Token_{AB} = Text_3 \,||\, e_{K_{AB}} \,(\, R_A \,||\, R_B \,||\, I_B \,||\, Text_2 \,)$$

$$Token_{BA} = Text_5 \,||\, e_{K_{AB}} \,(\, R_B \,||\, R_A \,||\, Text_4 \,)$$

The inclusion of the distinguishing identifier I_B in $Token_{AB}$ is optional.

NOTE When present, distinguishing identifier I_B is included in $Token_{AB}$ 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 I_B is made optional so that, in environments where such attacks cannot occur, it may be omitted. The distinguishing identifier I_B may also be omitted if unidirectional keys (see below) are used.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

The following is a description of Mechanism 4 — Three-pass authentication:

(1) *B* generates a random number R_B and sends it and, optionally, a text field $Text_1$ 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 deciphering the enciphered part [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifier I_B, if present, and that the random number R_B, sent to *A* in step (1), agrees with the random number contained in $Token_{AB}$.

(4) *B* generates and sends $Token_{BA}$ to *A*.

(5) On receipt of the message containing $Token_{BA}$, *A* verifies $Token_{BA}$ by deciphering the enciphered part [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking that the random number R_B, received from *B* in step (1) agrees with the random number contained in $Token_{BA}$ and that the random number R_A, sent to *B* in step (2), agrees with the random number contained in $Token_{BA}$.

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 (5).

7 Mechanisms involving a trusted third party

The authentication mechanisms in this Clause do not make use of a secret key shared by the two entities prior to the authentication process. They do, however, make use of a trusted third party (denoted by *P*) with which the entities *A* and *B* each share a secret key, K_{AP} and K_{BP} respectively. In both mechanisms one of the entities requests a key K_{AB} from the trusted third party. This is followed by an adaptation of the mechanisms described in 6.2.1 and 6.2.2, respectively.

As described below certain passes may be omitted from each mechanism if only unilateral authentication is required.

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 B for information on the use of text fields.

7.1 Mechanism 5 — Four-pass authentication

This mechanism is equivalent to Key Establishment Mechanism 8 of ISO/IEC 11770-2:2008.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

© ISO/IEC 2008 – All rights reserved

The authentication mechanism is illustrated in Figure 5.

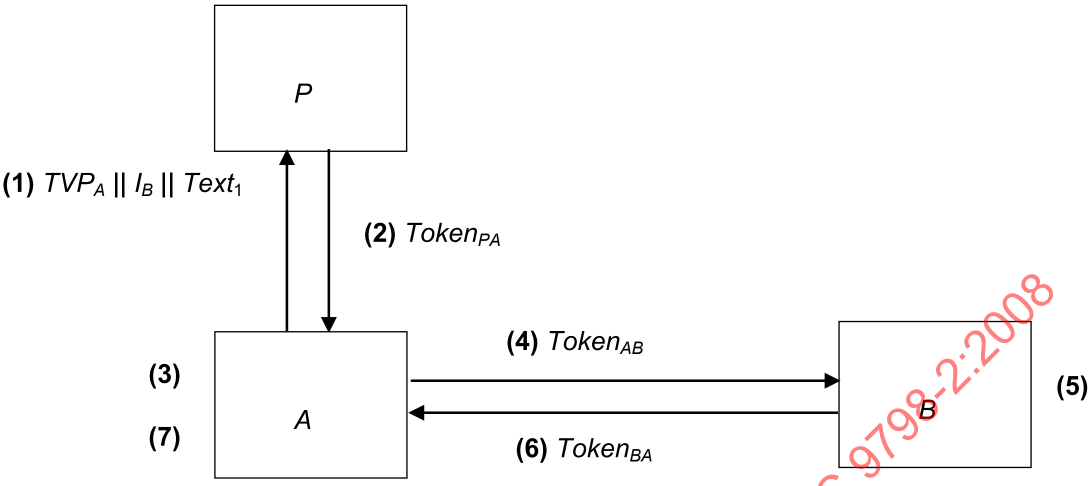

Figure 5 — Mechanism 5 — Four-pass authentication

The form of the token ($Token_{PA}$), sent by P to A, is:

$$Token_{PA} = Text_4 \,||\, e_{K_{AP}}(TVP_A \,||\, K_{AB} \,||\, I_B \,||\, Text_3) \,||\, e_{K_{BP}}(TN_P \,||\, K_{AB} \,||\, I_A \,||\, Text_2)$$

The form of the token ($Token_{AB}$), sent by A to B, is:

$$Token_{AB} = Text_6 \,||\, e_{K_{BP}}(TN_P \,||\, K_{AB} \,||\, I_A \,||\, Text_2) \,||\, e_{K_{AB}}(TN_A \,||\, I_B \,||\, Text_5)$$

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

$$Token_{BA} = Text_8 \,||\, e_{K_{AB}}(TN_B \,||\, I_A \,||\, Text_7)$$

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

The use of the time variant parameter TVP_A in steps (1) through (3) of Figure 5, as specified below, is somewhat different from its normal use. It allows A to associate the response message (2) with the message request (1). The important property of the time variant parameter here is its non-repeatability, to limit the possible reuse of a previously used $Token_{PA}$.

NOTE The time variant parameter TVP_A could be a random number. However, unlike the random numbers used in certain of the mechanisms in this part of ISO/IEC 9798, it is not necessary that TVP_A be unpredictable to a third party, and a non-repeating counter value would be equally appropriate.

The following is a description of Mechanism 5 — Four-pass authentication:

(1) A generates a time variant parameter TVP_A, and sends it, the distinguishing identifier I_B and, optionally, a text field $Text_1$ to the trusted third party P.

(2) The trusted third party P generates and sends $Token_{PA}$ to A.

(3) On receipt of the message containing $Token_{PA}$, A verifies $Token_{PA}$ by deciphering the data enciphered under K_{AP} [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifier I_B and that the time variant parameter, sent to P in

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

© ISO/IEC 2008 – All rights reserved

step (1), agrees with the time variant parameter contained in $Token_{PA}$. In addition, A retrieves the secret authentication key K_{AB}. A then extracts

$$e_{K_{BP}} (TN_P \,||\, K_{AB} \,||\, I_A \,||\, Text_2)$$

from $Token_{PA}$ and uses it to construct $Token_{AB}$.

(4) A generates and sends $Token_{AB}$ to B.

(5) On receipt of the message containing $Token_{AB}$, B verifies $Token_{AB}$ by deciphering the enciphered parts [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifiers I_A and I_B as well as the time stamp(s) or the sequence number(s). In addition, B retrieves the secret authentication key K_{AB}.

(6) B generates and sends $Token_{BA}$ to A.

(7) On receipt of the message containing $Token_{BA}$, A verifies $Token_{BA}$ by deciphering the enciphered part [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifier I_A as well as the time stamp or the sequence number.

Steps **(6)** and **(7)** may be omitted if only unilateral authentication of A to B is required.

7.2 Mechanism 6 — Five-pass authentication

In this mutual authentication mechanism uniqueness/timeliness is controlled by using random numbers (see Annex B of ISO/IEC 9798-1:1997). This mechanism is equivalent to Key Establishment Mechanism 9 of ISO/IEC 11770-2:2008.

The authentication mechanism is illustrated in Figure 6.

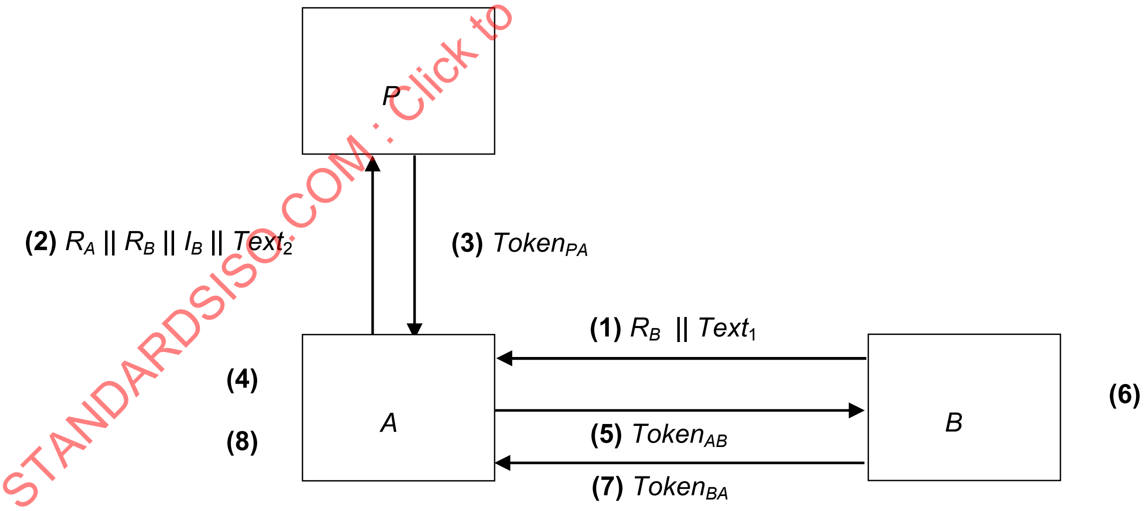

Figure 6 — Mechanism 6 — Five-pass authentication

The form of the token ($Token_{PA}$), sent by P to A, is:

$$Token_{PA} = Text_5 \,||\, e_{K_{AP}} (R_A \,||\, K_{AB} \,||\, I_B \,||\, Text_4) \,||\, e_{K_{BP}} (R_B \,||\, K_{AB} \,||\, I_A \,||\, Text_3)$$

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

© ISO/IEC 2008 – All rights reserved

The form of the token ($Token_{AB}$), sent by A to B, is:

$$Token_{AB} = Text_7 \,||\, e_{K_{BP}}\ (R_B \,||\, K_{AB} \,||\, I_A \,||\, Text_3) \,||\, e_{K_{AB}} (R'_A \,||\, R_B \,||\, Text_6)$$

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

$$Token_{BA} = Text_9 \,||\, e_{K_{AB}} (R_B \,||\, R'_A \,||\, Text_8)$$

The following is a description of Mechanism 6 — Five-pass authentication:

(1) B generates a random number R_B and sends it and, optionally, a text field $Text_1$ to A.

(2) A generates a random number R_A and sends it, the random number R_B, the distinguishing identifier I_B and, optionally, a text field $Text_2$ to the trusted third party P.

(3) The trusted third party P generates and sends $Token_{PA}$ to A.

(4) On receipt of the message containing $Token_{PA}$, A verifies $Token_{PA}$ by deciphering the data enciphered under K_{AP} [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifier I_B and that the random number R_A, sent to P in step (2), agrees with the random number contained in $Token_{PA}$. In addition, A retrieves the secret authentication key K_{AB}. A then extracts

$$e_{K_{BP}} (R_B \,||\, K_{AB} \,||\, I_A \,||\, Text_3)$$

from $Token_{PA}$ and uses it to construct $Token_{AB}$.

(5) A generates a second random number R'_A, and generates and sends $Token_{AB}$ to B.

(6) On receipt of the message containing $Token_{AB}$, B verifies $Token_{AB}$ by deciphering the enciphered parts [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking the correctness of the distinguishing identifier I_A and that the random number R_B, sent to A in step (1), agrees with both copies contained in $Token_{AB}$. In addition, B retrieves the secret authentication key K_{AB}.

(7) B generates and sends $Token_{BA}$ to A.

(8) On receipt of the message containing $Token_{BA}$, A verifies $Token_{BA}$ by deciphering the enciphered part [where deciphering implies that the requirements given in Clause 5 d) are met] and then checking that the random number R_B, received from B in step (1), agrees with the random number contained in $Token_{BA}$ and that the random number R'_A, sent to B in step (5), agrees with the random number contained in $Token_{BA}$.

Steps (7) and (8) may be omitted if only unilateral authentication of A to B is required.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

Annex A
(normative)

OIDs and ASN.1 syntax

A.1 Formal definition

```
EntityAuthenticationMechanisms-2 {

   iso(1) standard(0) e-auth-mechanisms(9798) part2(2)

      asn1-module(0) object-identifiers(0) }

   DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

-- IMPORTS None; --

OID ::= OBJECT IDENTIFIER -- alias

-- Synonyms --

is9798-2 OID ::= { iso(1) standard(0) e-auth-mechanisms(9798) part2(2) }

mechanism OID ::= { is9798-2 mechanisms(1) }

-- Unilateral and mutual entity authentication mechanisms not involving a trusted
third party --

ua-one-pass OID ::= { mechanism 1 }

ua-two-pass OID ::= { mechanism 2 }

ma-two-pass OID ::= { mechanism 3 }

ma-three-pass OID ::= { mechanism 4 }

-- Mutual entity authentication mechanisms involving a trusted third party --

ttp-ma-four-pass OID ::= { mechanism 5 }

ttp-ma-five-pass OID ::= { mechanism 6 }

END -- EntityAuthenticationMechanisms-2 --
```

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008

A.2 Use of subsequent object identifiers

Each of the entity authentication mechanisms uses a symmetric encryption technique. Therefore, the entity authentication mechanism object identifier may be followed by an object identifier specifying the encryption technique used, for example an identifier for one of the mechanisms specified in ISO/IEC 19772.

© ISO/IEC 2008 – All rights reserved

A.3 Coding examples in accordance with the basic encoding rules of ASN.1

In accordance with ISO/IEC 8825-1, an object identifier consists of one or more series of octets. Each series encodes a number.

— Bit 8 (the most significant bit) is set equal to zero in the last octet of a series and to one in the previous octets, if there is more than one octet.

— The concatenation of bits 7 to 1 of the octets of a series encodes a number. Each number shall be encoded using the fewest possible octets, that is, the octet '80' is invalid in the first position of a series.

— The first number is the number of the standard; the second number, if present, is the part in a multi-part standard.

An object identifier may refer to any mechanism defined in this document.

— To identify an ISO standard, the first octet is set equal to '28', i.e., 40 in decimal (see ISO/IEC 8825-1).

— The next two octets are set equal to 'CC46'. 9798 is equal to '2646' in hexadecimal, i.e., 0010 0110 0100 0110, i.e., two blocks of seven bits: 1001100 1000110. After insertion of the appropriate value of bit 8 in each octet, the encoding of the series is therefore 11001100 01000110, i.e., 'CC46'.

— The next octet is set equal to '02' to identify part 2.

— The next octet identifies an authentication mechanism.

— '01' identifies the one-pass unilateral authentication mechanism not involving a trusted third party.

— '02' identifies the two-pass unilateral authentication mechanism not involving a trusted third party.

— '03' identifies the two-pass mutual authentication mechanism not involving a trusted third party.

— '04' identifies the three-pass mutual authentication mechanism not involving a trusted third party.

— '05' identifies the four-pass mutual authentication mechanism involving a trusted third party.

— '06' identifies the five-pass mutual authentication mechanism involving a trusted third party.

For example, the data element '28 CC 46 02 05' reads {iso standard 9798 2 5}, i.e., the fifth mechanism in ISO/IEC 9798-2, i.e., the four-pass mutual authentication mechanism involving a trusted third party. The data element may be conveyed in the following BER-TLV data object (see the basic encoding rules of ASN.1, ISO/IEC 8825-1, universal class tag '06') where the dashes and the curly brackets are not significant, and are inserted for clarity only.

Data object = {'06'-'05'-'28 CC 46 02 05'}

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 9798-2:2008