



BSI Standards Publication

IT Security techniques — Entity authentication

Part 2: Mechanisms using authenticated encryption

National foreword

This British Standard is the UK implementation of [ISO/IEC 9798-2:2019](#). It supersedes [BS ISO/IEC 9798-2:2008](#), which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 580 51051 9

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2019.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

INTERNATIONAL STANDARD

BS ISO/IEC 9798-2:2019

ISO/IEC 9798-2

Fourth edition
2019-06-26

IT Security techniques — Entity authentication —

Part 2: Mechanisms using authenticated encryption

*Techniques de sécurité IT — Authentification d'entité —
Partie 2: Mécanismes utilisant le chiffrement authentifié*



Reference number
ISO/IEC 9798-2:2019(E)

© ISO/IEC 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	2
5 General	3
6 Requirements	3
7 Mechanisms not involving an on-line trusted third party	4
7.1 General.....	4
7.2 Unilateral authentication.....	4
7.2.1 General.....	4
7.2.2 Mechanism UNI.TS — One-pass authentication.....	5
7.2.3 Mechanism UNI.CR — Two-pass authentication.....	5
7.3 Mutual authentication.....	6
7.3.1 General.....	6
7.3.2 Mechanism MUT.TS — Two-pass authentication.....	6
7.3.3 Mechanism MUT.CR — Three-pass authentication.....	7
8 Mechanisms involving an on-line trusted third party	8
8.1 General.....	8
8.2 Mechanism TP.TS — Four-pass authentication.....	8
8.3 Mechanism TP.CR — Five-pass authentication.....	10
Annex A (normative) Object Identifiers	12
Annex B (informative) Use of text fields	13
Annex C (informative) Properties of entity authentication mechanisms	14
Bibliography	15

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This fourth edition cancels and replaces the third edition ([ISO/IEC 9798-2:2008](http://www.iso.org/iso/9798-2:2008)), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 9798-2:2008/Cor.1:2010, ISO/IEC 9798-2:2008/Cor.2:2012 and ISO/IEC 9798-2:2008/Cor.3:2013. The main changes compared to the previous edition are as follows:

- replacement of encryption by authenticated encryption;
- inclusion of constants uniquely identifying the mechanism and the instance of authenticated encryption within the mechanism.

A list of all parts in the ISO/IEC 9798 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

IT Security techniques — Entity authentication —

Part 2: Mechanisms using authenticated encryption

1 Scope

This document specifies entity authentication mechanisms using authenticated encryption 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 an on-line trusted third party for the establishment of a common secret key. They also realize mutual or unilateral entity authentication.

[Annex A](#) defines Object Identifiers for the mechanisms specified in this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1 authenticated encryption

(reversible) transformation of data by a cryptographic algorithm to produce *ciphertext* (3.2) that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, data integrity, and data origin authentication

[SOURCE: ISO/IEC 19772:2009, 3.1]

3.2 ciphertext

data which has been transformed to hide its information content

[SOURCE: ISO/IEC 10116:2017, 3.2]

3.3 claimant

entity that is, or represents, a principal for the purposes of authentication

3.4 time stamp

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

[SOURCE: ISO/IEC 18014-1:2008, 3.12]

3.5 trusted third party TTP

security authority, or its agent, trusted by other entities with respect to security related activities

[SOURCE: ISO/IEC 18014-1:2008, 3.20]

4 Symbols and abbreviated terms

A, B	Labels used for the entities participating in a mechanism.
d_K	An authenticated decryption process using secret key K .
e_K	An authenticated encryption process performed using secret key K .
$e_K(X)$	The result of the encryption process for data X with an authenticated encryption algorithm using a key K .
I_U	A distinguishing identifier of entity U .
K	A secret key used with the encryption and decryption processes.
K_{UV}	A secret key shared between entities U and V used only in authenticated encryption 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 .
SID_m^i	Constant uniquely identifying the mechanism m and the instance of authenticated encryption (number i) within the mechanism.
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 .
$X Y$	The result of the concatenation of data items X and Y in the order specified. In cases where the result of concatenating two or more data items is encrypted as part of one of the mechanisms specified in this document, this result shall be composed so that it can be uniquely resolved into its constituent data strings, i.e. so that there is no possibility of ambiguity in interpretation.

NOTE This latter property can be achieved in a variety of ways, depending on the application. For example, it can be guaranteed by a) fixing the length of each of the substrings throughout the domain of use of the mechanism, or b) encoding the sequence of concatenated strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1[2].

5 General

In the authentication mechanisms specified in this document, 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 encrypt specific data. The encrypted data can be decrypted by anyone sharing the entity's secret authentication key. The decrypted data shall include a time variant parameter. The parameter can be verified in the following ways.

- a) If it is a random number, then the recipient should make sure it is identical to the random challenge previously sent to the claimant. For guidance on the creation and use of random numbers, see [ISO/IEC 18031](#).
- b) If it is a time stamp, the recipient should verify the validity of the time stamp. Guidance on the use and verification of time stamps is provided in [ISO/IEC 9798-1:2010](#), Annex B.
- c) If it is a sequence number, then the recipient shall be able to compare it with previously received or stored sequence number(s) to make sure it is not a replay. Guidance on the use and verification of sequence numbers is provided in [ISO/IEC 9798-1:2010](#), Annex B.

The mechanisms specified in this document 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, the additional communication between an entity and the trusted third party requires two extra passes in the communication exchange.

[Annex A](#) defines the Object Identifiers which shall be used to identify the mechanisms specified in this document. [Annex B](#) shows the information on the use of text fields. [Annex C](#) shows the main properties of the entity authentication mechanisms specified in this document.

6 Requirements

The authentication mechanisms have the following requirements. If any of these is not met, then the authentication process can be compromised or not implementable.

- 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 7](#) apply, or each entity shall share a secret authentication key with a common trusted third party, in which case the mechanisms of [Clause 8](#) apply. Such keys shall be known to the involved parties prior to the beginning of any particular occurrence of an authentication mechanism. The method by which this is achieved is beyond the scope of this document. 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 1 The authenticated encryption algorithm and the key lifetime must be chosen so that it is computationally infeasible for a key to be deduced during its lifetime. In addition, the key lifetime must be chosen to prevent known plaintext or chosen plaintext attacks.

- d) The tokens used in the mechanisms shall be unforgeable even with the knowledge of old tokens. In other words, old tokens shall not be reusable in any way (in part or in full) to construct new tokens. For every possible secret key, K , the authenticated encryption function, e_K , and its corresponding

decryption function, d_K , shall have the following property. The decryption 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 are “accepted” when subjected to the decryption process, d_K .

NOTE 2 In practice, this can be achieved in many ways. The most common approach is to use the secret key, K , with an authenticated encryption technique that provides both confidentiality and integrity protection, as standardized in [ISO/IEC 19772](#).

- e) The mechanisms in this document 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 [ISO/IEC 9798-1:2010](#), Annex B.
- f) The secret authentication key used in implementations of any of the mechanisms specified in this document shall be distinct from keys used for any other purposes.
- g) The data strings decrypted at various points in an authentication mechanism shall not be composed so that they can be interchanged. To help achieve this requirement, the mechanisms in this document include constants SID_m^i in the encrypted data. The recipient shall verify that the constant SID_m^i in the authenticated encrypted data is as expected.

NOTE 3 The form of the constants is not specified in this document. However, in order to meet the requirement, they can be defined to include the following data elements:

- the object identifier as specified in [Annex A](#), in particular identifying the ISO/IEC standard number and the authentication mechanism;
- a constant that uniquely identifies the authenticated encrypted string within the mechanism. This constant can be omitted in mechanisms that include only one signed string.
- h) In the mechanisms specified in [Clause 8](#), the holder of a key K_{AP} (or K_{BP}) shall always use it in the same way, i.e. acting either as the TTP P or as the entity A (or B). That is, no entity shall act as the TTP in one instance of a protocol and act as A or B in another instance of the protocol, and use the same key in both cases.
- i) The initialization vector (IV) for the authenticated encryption algorithm shall be generated according to the requirements of that algorithm. In many cases this implies that the IV should be unique across multiple executions of the authenticated encryption algorithm performed using the same key.

7 Mechanisms not involving an on-line trusted third party

7.1 General

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, entity A always uses the unidirectional key, K_{AB} , for encryption, while B always uses it to decrypt (and conversely for key, K_{BA}).

All text fields specified in the following mechanisms are available for use in applications outside the scope of this document (they may be empty). Their relationship and contents depend on the specific application. See [Annex B](#) for information on the use of text fields.

7.2 Unilateral authentication

7.2.1 General

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

7.2.2 Mechanism UNI.TS — 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 [ISO/IEC 9798-1:2010](#), Annex B). The authentication mechanism is illustrated in [Figure 1](#).

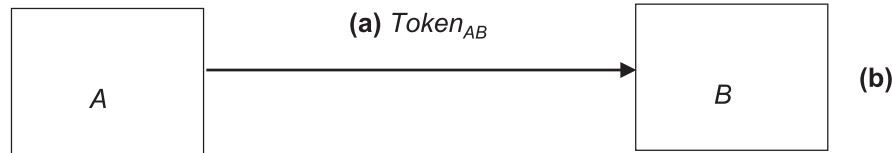


Figure 1 — Mechanism UNI.TS — One-pass authentication

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

$$Token_{AB} = Text_2 \parallel e_{K_{AB}} \left(SID_{UNI.TS}^1 \parallel TN_A \parallel I_B \parallel Text_1 \right)$$

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 it can be omitted in environments where such attacks cannot occur. The distinguishing identifier, I_B , can also be omitted if a unidirectional key is used.

The following is a description of Mechanism UNI.TS — One-pass authentication:

- a) *A* generates and sends $Token_{AB}$ to *B*.
- b) On receipt of the message containing $Token_{AB}$, *B* verifies $Token_{AB}$ by decrypting the encrypted part in the authenticated mode and by checking the SID . Next, *B* checks the correctness of the distinguishing identifier, I_B , if present, as well as the time stamp or the sequence number.

7.2.3 Mechanism UNI.CR — 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 [ISO/IEC 9798-1:2010](#), Annex B). The authentication mechanism is illustrated in [Figure 2](#).

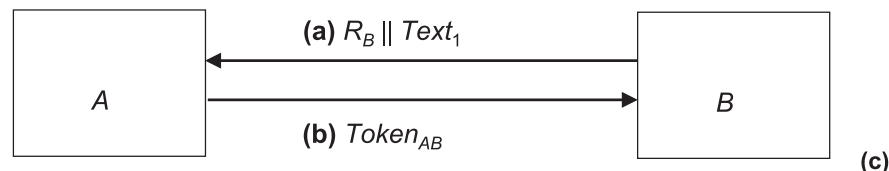


Figure 2 — Mechanism UNI.CR — Two-pass authentication

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

$$Token_{AB} = Text_3 \parallel e_{K_{AB}} \left(SID_{UNI.CR}^1 \parallel R_B \parallel I_B \parallel Text_2 \right)$$

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

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 can include a random number R_A in $Text_2$.

NOTE 2 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 . The inclusion of the distinguishing identifier I_B is made optional so that it can be omitted in environments where such attacks cannot occur. The distinguishing identifier, I_B , can also be omitted if a unidirectional key is used.

The following is a description of Mechanism UNI.CR — Two-pass authentication:

- a) B generates a random number R_B and sends it and, optionally, a text field $Text_1$ to A .
- b) A generates and sends $Token_{AB}$ to B .
- c) On receipt of the message containing $Token_{AB}$, B verifies $Token_{AB}$ by decrypting the encrypted part in the authenticated mode and by checking the SID . Next, B checks the correctness of the distinguishing identifier, I_B , if present, and that the random number, R_B , sent to A in step a), agrees with the random number contained in $Token_{AB}$.

7.3 Mutual authentication

7.3.1 General

Mutual authentication means that the two communicating entities are authenticated to each other by use of the mechanism.

The mechanisms described in 7.2.2 and 7.2.3 are adapted in 7.3.2 and 7.3.3, respectively, to achieve mutual authentication. In both cases, this requires one more pass and results in two more steps.

7.3.2 Mechanism MUT.TS — Two-pass authentication

In this authentication mechanism, uniqueness/timeliness is controlled by generating and checking time stamps or sequence numbers (see ISO/IEC 9798-1:2010, Annex B).

The authentication mechanism is illustrated in Figure 3.



Figure 3 — Mechanism MUT.TS — Two-pass authentication

The form of the token, $Token_{AB}$, sent by A to B , is identical to that specified in 7.2.2:

$$Token_{AB} = Text_2 \parallel e_{K_{AB}} \left(SID_{MUT.TS}^1 \parallel TN_A \parallel I_B \parallel Text_1 \right)$$

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

$$Token_{BA} = Text_4 \parallel e_{K_{AB}} \left(SID_{MUT.TS}^2 \parallel TN_A \parallel TN_B \parallel I_A \parallel Text_3 \right)$$

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.

NOTE 1 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 one or both can be omitted in environments where such attacks cannot occur. The distinguishing identifiers, I_A and I_B , can also be omitted if unidirectional keys (see below) are used.

NOTE 2 If the required TN_A were to be omitted in $Token_{BA}$, the two messages of this mechanism would not be bound together in any way, other than implicitly by timeliness. The mechanism no longer achieves mutual authentication.

NOTE 3 Text1 cannot be reliably authenticated if A reuses TN_A . A should thus always use a unique TN_A in every session.

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 MUT.TS — Two-pass authentication:

- a) A generates and sends $Token_{AB}$ to B .
- b) On receipt of the message containing $Token_{AB}$, B verifies $Token_{AB}$ by decrypting the encrypted part in the authenticated mode and by checking the SID . Next, B checks the correctness of the distinguishing identifier I_B , if present, as well as the time stamp or the sequence number.
- c) B generates and sends $Token_{BA}$ to A .
- d) On receipt of the message containing $Token_{BA}$, A verifies $Token_{BA}$ by decrypting the encrypted part in the authenticated mode and by checking the SID . Next, A checks the correctness of the distinguishing identifier I_A , if present, as well as the time stamp or the sequence number. A also verifies that the received TN_A is identical to the one sent in $Token_{AB}$.

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 d).

7.3.3 Mechanism MUT.CR — Three-pass authentication

In this authentication mechanism, uniqueness/timeliness is controlled by generating and checking random numbers (see ISO/IEC 9798-1:2010, Annex B).

The authentication mechanism is illustrated in Figure 4.

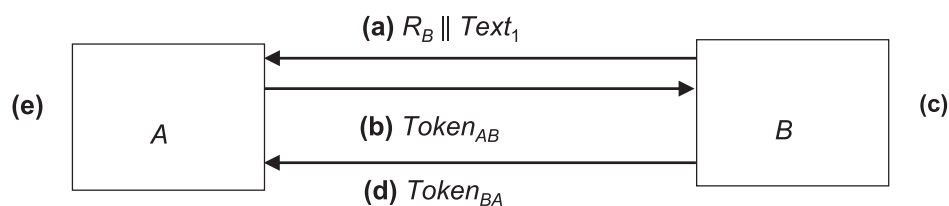


Figure 4 — Mechanism MUT.CR — Three-pass authentication

The tokens are of the following form:

$$\text{Token}_{AB} = \text{Text}_3 \parallel e_{K_{AB}} \left(\text{SID}_{\text{MUT.CR}}^1 \parallel R_A \parallel R_B \parallel I_B \parallel \text{Text}_2 \right)$$

$$\text{Token}_{BA} = \text{Text}_5 \parallel e_{K_{AB}} \left(\text{SID}_{\text{MUT.CR}}^2 \parallel R_A \parallel I_B \parallel \text{Text}_4 \right)$$

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 . The inclusion of the distinguishing identifier I_B is made optional so that it can be omitted in environments where such attacks cannot occur. The distinguishing identifier, I_B , can also be omitted if unidirectional keys (see below) are used.

The following is a description of Mechanism MUT.CR — Three-pass authentication:

- a) B generates a random number, R_B , and sends it and, optionally, a text field Text_1 to A .
- b) A generates a random number, R_A , and generates and sends Token_{AB} to B .
- c) On receipt of the message containing Token_{AB} , B verifies Token_{AB} by decrypting the encrypted part in the authenticated mode and by checking the SID . Next, B checks the correctness of the distinguishing identifier, I_B , if present, and that the random number, R_B , sent to A in step a), agrees with the random number contained in Token_{AB} .
- d) B generates and sends Token_{BA} to A .
- e) On receipt of the message containing Token_{BA} , A verifies Token_{BA} by decrypting the encrypted part in the authenticated mode and by checking the SID . Next, A checks that the random number, R_A , sent to B in step b), 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 e).

8 Mechanisms involving an on-line trusted third party

8.1 General

The authentication mechanisms in [Clause 8](#) 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 [7.3.2](#) and [7.3.3](#), respectively.

NOTE If unidirectional keys are used, requirement h) in [Clause 6](#) is automatically satisfied. However, if bidirectional keys are used, this requirement can be enforced through policy rules external to the mechanism itself.

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 document (they can be empty). Their relationship and contents depend on the specific application. See [Annex B](#) for information on the use of text fields.

8.2 Mechanism TP.TS — Four-pass authentication

The authentication mechanism is illustrated in [Figure 5](#).

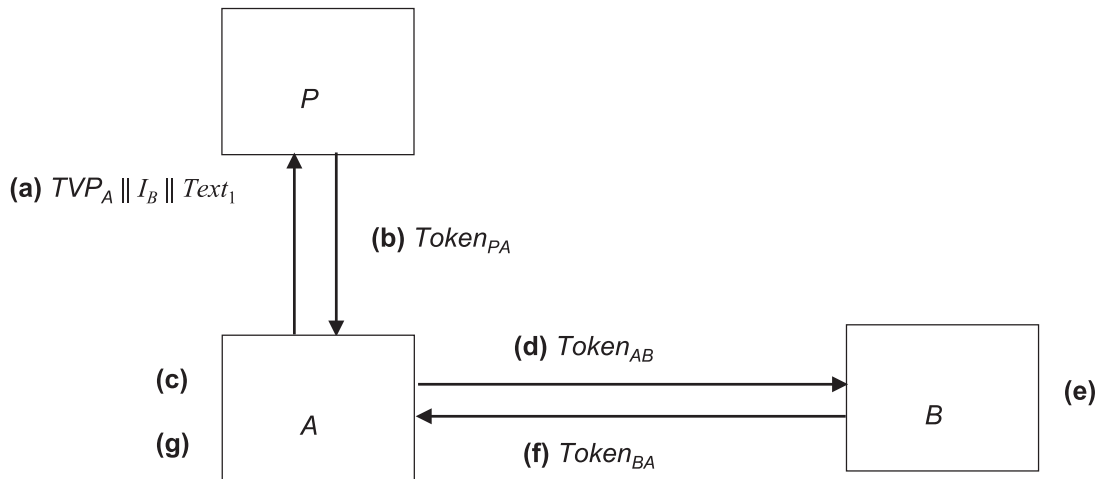


Figure 5 — Mechanism TP.TS — Four-pass authentication

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

$$Token_{PA} = Text_4 || e_{K_{AP}} \left(SID_{TP.TS}^1 || TVP_A || K_{AB} || I_B || Text_3 \right) || e_{K_{BP}} \left(SID_{TP.TS}^2 || TN_P || K_{AB} || I_A || Text_2 \right)$$

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

$$Token_{AB} = Text_6 || e_{K_{BP}} \left(SID_{TP.TS}^2 || TN_P || K_{AB} || I_A || Text_2 \right) || e_{K_{AB}} \left(SID_{TP.TS}^3 || TN_A || Text_5 \right)$$

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

$$Token_{BA} = Text_8 || e_{K_{AB}} \left(SID_{TP.TS}^4 || TN_B || Text_7 \right)$$

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 a) to c) of [Figure 5](#), as specified below, is somewhat different from its normal use. It allows A to associate the response message b) with the message request a). 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 can be a random number. However, unlike the random numbers used in certain of the mechanisms in this document, 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 TP.TS — Four-pass authentication:

- A generates a time variant parameter TVP_A , and sends it, along with the distinguishing identifier, I_B , and, optionally, a text field, $Text_1$, to the trusted third party, P .
- The trusted third party, P , generates a random key, K_{AB} , and generates and sends $Token_{PA}$ to A .
- On receipt of the message containing $Token_{PA}$, A verifies $Token_{PA}$ by decrypting the data encrypted under K_{AP} in the authenticated mode and by checking the SID . Next, A checks the correctness of the distinguishing identifier, I_B , and that the time variant parameter, sent to P in step a), agrees with the time variant parameter contained in $Token_{PA}$. In addition, A retrieves the secret authentication key K_{AB} . A then extracts $e_{K_{BP}} \left(SID_{TP.TS}^2 || TN_P || K_{AB} || I_A || Text_2 \right)$ from $Token_{PA}$ and uses it to construct $Token_{AB}$.

- d) *A* generates and sends $Token_{AB}$ to *B*.
- e) On receipt of the message containing $Token_{AB}$, *B* verifies $Token_{AB}$ by decrypting the encrypted parts in the authenticated mode and by checking the *SID*. Next, *B* checks the correctness of the distinguishing identifier I_A as well as the time stamp(s) or the sequence number(s). In addition, *B* retrieves the secret authentication key K_{AB} .
- f) *B* generates and sends $Token_{BA}$ to *A*.
- g) On receipt of the message containing $Token_{BA}$, *A* verifies $Token_{BA}$ by decrypting the encrypted part in the authenticated mode, by checking the *SID*, and then checking the correctness of the time stamp or the sequence number.

Steps f) and g) may be omitted if only unilateral authentication of *A* to *B* is required.

8.3 Mechanism TP.CR — Five-pass authentication

In this mutual authentication mechanism, uniqueness/timeliness is controlled by using random numbers (see [ISO/IEC 9798-1:2010](#), Annex B). The authentication mechanism is illustrated in [Figure 6](#).

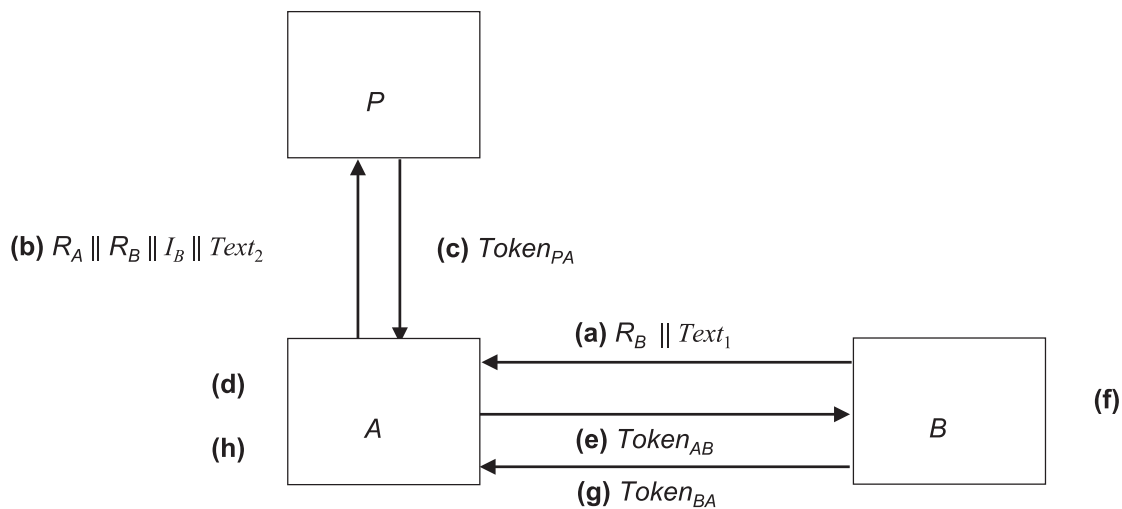


Figure 6 — Mechanism TP.CR — Five-pass authentication

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

$$Token_{PA} = Text_5 || e_{K_{AP}} \left(SID_{TP.CR}^1 || R_A || K_{AB} || I_B || Text_4 \right) || e_{K_{BP}} \left(SID_{TP.CR}^2 || R_B || K_{AB} || I_A || Text_3 \right)$$

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

$$Token_{AB} = Text_7 || e_{K_{BP}} \left(SID_{TP.CR}^2 || R_B || K_{AB} || I_A || Text_3 \right) || e_{K_{AB}} \left(SID_{TP.CR}^3 || R'_A || R_B || Text_6 \right)$$

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

$$Token_{BA} = Text_9 || e_{K_{AB}} \left(SID_{TP.CR}^4 || R'_A || Text_8 \right)$$

The following is a description of Mechanism TP.CR — Five-pass authentication:

- a) *B* generates a random number, R_B , and sends it and, optionally, a text field, $Text_1$, to *A*.
- b) *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*.

- c) The trusted third party, P , generates a random key, K_{AB} , and generates and sends $Token_{PA}$ to A .
- d) On receipt of the message containing $Token_{PA}$, A verifies $Token_{PA}$ by decrypting the data encrypted under K_{AP} in the authenticated mode and by checking the SID . Next, A checks the correctness of the distinguishing identifier, I_B , and that the random number R_A , sent to P in step b), agrees with the random number contained in $Token_{PA}$. In addition, A retrieves the secret authentication key, K_{AB} . A then extracts $e_{K_{BP}} \left(SID_{TP,CR}^2 \parallel R_B \parallel K_{AB} \parallel I_A \parallel Text_3 \right)$ from $Token_{PA}$ and uses it to construct $Token_{AB}$.
- e) A generates a second random number, R'_A , and generates and sends $Token_{AB}$ to B .
- f) On receipt of the message containing $Token_{AB}$, B verifies $Token_{AB}$ by decrypting the encrypted parts in the authenticated mode and by checking the SID . Next, B checks the correctness of the distinguishing identifier, I_A , and that the random number, R_B , sent to A in step a), agrees with both copies contained in $Token_{AB}$. In addition, B retrieves the secret authentication key, K_{AB} .
- g) B generates and sends $Token_{BA}$ to A .
- h) On receipt of the message containing $Token_{BA}$, A verifies $Token_{BA}$ by decrypting the encrypted part in the authenticated mode and by checking the SID . Next, A checks that the random number, R'_A , sent to B in step e), agrees with the random number contained in $Token_{BA}$.

Steps g) and h) may be omitted if only unilateral authentication of A to B is required.

Annex A (normative)

Object Identifiers

[Annex A](#) defines Object Identifiers for the mechanisms specified in this document.

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-2019(2) }

/*
Unilateral and mutual entity authentication mechanisms not involving a
trusted third party
*/
nottp-mechanism OID ::= { mechanism nottp(1) }
nottp-uni-mechanism OID ::= { nottp-mechanism uni(1) }
nottp-mut-mechanism OID ::= { nottp-mechanism mut(2) }
uni-ts OID ::= { nottp-uni-mechanism 1 }
uni-cr OID ::= { nottp-uni-mechanism 2 }
mut-ts OID ::= { nottp-mut-mechanism 1 }
mut-cr OID ::= { nottp-mut-mechanism 2 }

-- Mutual entity authentication mechanisms involving a trusted third
party --
ttp-mechanism OID ::= { mechanism ttp(2) }
ttp-mut-1 OID ::= { ttp-mechanism 1 }
ttp-mut-2 OID ::= { ttp-mechanism 2 }

END -- EntityAuthenticationMechanisms-2 --
```

A.2 Use of subsequent object identifiers

Each of the entity authentication mechanisms uses a symmetric authenticated 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](#) and any associated parameters (e.g. the block cipher encryption mechanism identifier, the block cipher mode of operation and/or MAC algorithm as further specified in [ISO/IEC 19772](#)).

Annex B **(informative)**

Use of text fields

The tokens specified in [Clauses 7](#) and [8](#) contain text fields. The actual use of and relationships between the various text fields in a given pass depend on the application. An example is given below; see also [ISO/IEC 9798-1:2010](#), Annex A.

Any information requiring confidentiality or data origin authentication should be placed in the encrypted part of the token.

Encrypted text fields may be used to indicate that the token is only valid for the purpose of entity authentication. If there is a concern that one entity can choose a “degenerate” value with malicious intent for the other entity to encrypt, the other entity may introduce a random number in the text field.

Text fields can also be used to provide information to a verifier indicating the (unauthenticated) identity which a claimant is claiming. Such information can be required to allow a verifier to determine which key is to be used to authenticate a claimant.

Annex C (informative)

Properties of entity authentication mechanisms

[Table C.1](#) summarizes the main properties of the entity authentication mechanisms specified in this document. Options are shown in parentheses, e.g. mechanism TP.TS has an optional three-pass version of the protocol to achieve unilateral authentication.

Table C.1 — Properties of mechanisms

Mechanism	UNI.TS	UNI.CR	MUT.TS	MUT.CR	TP.TS	TP.CR
Number of passes	1	2	2	3	4 (or optional-ly 3)	5 (or optional-ly 4)
Unilateral/Mutual between Verifier and Claimant	Unilateral	Unilateral	Mutual	Mutual	Mutual (Unilateral)	Mutual (Unilateral)
Variable(s) which guarantees freshness (NOTE 1)	TN_A	R_B	TN_A and TN_B	R_A and R_B	TVP_A , TN_B and TN_P	R_A and R_B
Entity which initiates the (authentication) mechanism	A	B	A	B	A	B
Claimant knowledge of success (NOTE 2)	No	No	Only for A	Only for A	Only for A	Only for A

NOTE 1 For mechanisms UNI.CR, MUT.CR and TP.CR which use random number(s) to guarantee freshness, there is no need to maintain either synchronised clocks or sequence numbers between the two entities.

NOTE 2 In the authentication mechanisms described in this document, a claimant sends proof of identity in the form of an encrypted token. In some cases, there is no response from the other entity to indicate that the proof was successfully accepted. The last row of [Table C.1](#) indicates where the protocol inherently guarantees knowledge of successful authentication. In all other cases, the system needs to make provision for knowledge of success to the claimant if it is required.

Bibliography

- [1] ISO/IEC 8824 (all parts), *Information technology — Abstract Syntax Notation One (ASN.1)*
- [2] ISO/IEC 8825 (all parts), *Information technology — ASN.1 encoding*
- [3] [ISO/IEC 9797-1](#), *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*
- [4] [ISO/IEC 9798-5](#), *Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques*
- [5] [ISO/IEC 10116](#), *Information technology — Security techniques — Modes of operation for an n-bit block cipher*
- [6] [ISO/IEC 11770-1](#), *Information technology — Security techniques — Key management — Part 1: Framework*
- [7] [ISO/IEC 11770-2](#), *IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*
- [8] [ISO/IEC 18014-1](#), *Information technology — Security techniques — Time-stamping services — Part 1: Framework*
- [9] [ISO/IEC 18031](#), *Information technology — Security techniques — Random bit generation*
- [10] [ISO/IEC 19772](#), *Information technology — Security techniques — Authenticated encryption*
- [11] BASIN D., CREMERS C., MEIER S. Provably repairing the ISO/IEC 9798 standard for entity authentication'. In: P. Degano, J. D. Guttman (eds.), *Principles of Security and Trust - First International Conference, POST 2012, Tallinn, Estonia, March 24 - April 1, 2012, Proceedings*. Springer LNCS 7215, pp.129-148, 2012

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.
- Standards purchased in hard copy format:
- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services

Tel: +44 345 086 9001

Email (orders): orders@bsigroup.com

Email (enquiries): cservices@bsigroup.com

Subscriptions

Tel: +44 345 086 9001

Email: subscriptions@bsigroup.com

Knowledge Centre

Tel: +44 20 8996 7004

Email: knowledgecentre@bsigroup.com

Copyright & Licensing

Tel: +44 20 8996 7070

Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK