INTERNATIONAL STANDARD

ISO/IEC 9798-2

Fourth edition
2019-06

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

Published in Switzerland

Contents

Page

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), 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^i_{m}	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.
$X \mid\mid Y$	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^i_m in the encrypted data. The recipient shall verify that the constant SID^i_m 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.

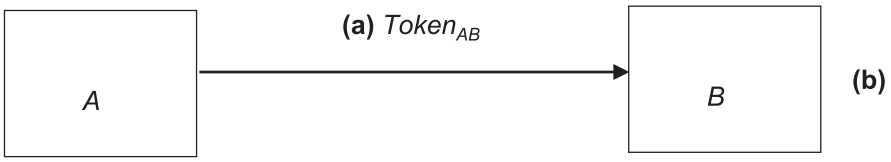

Figure 1 — Mechanism UNI.TS — One-pass authentication

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

$$\text{Token}_{AB} = \text{Text}_2 \,||\, e_{K_{AB}}\left(SID^1_{\text{UNI.TS}} \,||\, TN_A \,||\, I_B \,||\, \text{Text}_1\right)$$

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.

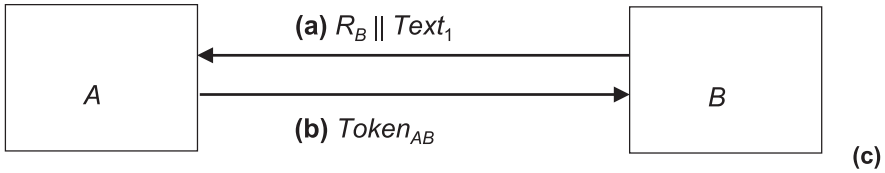

Figure 2 — Mechanism UNI.CR — Two-pass authentication

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

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

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