INTERNATIONAL STANDARD

ISO/IEC 9798-3

Third edition
2019-01

IT Security techniques — Entity authentication —

Part 3: Mechanisms using digital signature techniques

Techniques de sécurité IT — Authentification d'entité —

Partie 3: Mécanismes utilisant des techniques de signature numériques

Reference number
ISO/IEC 9798-3:2019(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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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 Joint Technical Committee JTC 1, *Information Technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 9798–3:1998), which has been technically revised. It also incorporates the amendment ISO/IEC 9798–3:1998/Amd 1:2010, and corrigenda ISO/IEC 9798–3:1998/Cor 1:2009 and ISO/IEC 9798–3:1998/Cor 2:2012. The main changes compared to the previous edition are as follows:

— all mechanisms have been technically revised to resolve security issues and make the mechanism secure by default;

— all mechanisms have been renamed and editorially improved to represent them more clearly;

— three additional mechanisms have been included using an on-line trusted third party;

— guidance to explain the security properties of the mechanisms and guide users in selecting the appropriate mechanism for their use case has been added (Annex B).

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 3:
Mechanisms using digital signature techniques

1 Scope

This document specifies entity authentication mechanisms using digital signatures based on asymmetric techniques. A digital signature is used to verify the identity of an entity.

Ten mechanisms are specified in this document. The first five mechanisms do not involve an on-line trusted third party and the last five make use of on-line trusted third parties. In both of these two categories, two mechanisms achieve unilateral authentication and the remaining three achieve mutual authentication.

Annex A defines the object identifiers assigned to the entity authentication 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*

ISO/IEC 14888 (all parts), *Information technology — Security techniques — Digital signatures with appendix*

ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery.*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
atomic transaction
transaction which cannot be split into multiple smaller transactions

3.2
claimant
entity which is or represents a principal for the purposes of authentication

[SOURCE: ISO/IEC 9798–1:2010, 3.6, modified — The Note to entry has been removed.]

3.3
digital signature
signature
data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to verify the source and integrity of the data unit

3.4
entity authentication
corroboration that an entity is the one claimed

[SOURCE: ISO/IEC 9798–1:2010, 3.14]

3.5
mutual authentication
entity authentication (3.4) which provides both entities with assurance of each other's identity

[SOURCE: ISO/IEC 9798–1:2010, 3.18]

3.6
token
message consisting of data fields that are the output of a cryptographic function

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

[SOURCE: ISO/IEC 9798–1:2010, 3.38, modified — The Note to entry has been removed.]

3.8
unilateral authentication
entity authentication which provides one entity with assurance of the other's identity but not vice versa

[SOURCE: ISO/IEC 9798–1:2010, 3.39]

3.9
verifier
entity that requires to verify the identity of another entity

4 Symbols and abbreviated terms

The symbols and abbreviated terms given in ISO/IEC 9798–1 and the following shall apply.

$Cert_X$	certificate for entity X
I_X	representation of the identity of entity X, which is either i_X or $Cert_X$
i_X	string identifying entity X
M	data string that is input to a digital signature algorithm
P_X	public verification key associated with X
Res_X	result of verifying entity X's public key or public key certificate
SID^i_m	constant uniquely identifying the mechanism m and the signed string (number i) within the mechanism
$sS_X(M)$	signature on data string M with the private signing key of entity X. The signature shall be such that M can be recovered

$\frac{T_X}{N_X}$ time variant parameter used by entity X, either a sequence number N_X or a time stamp T_X

$X \| Y$ 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 signed as part of one of the mechanisms specified in this document, this result should 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 Unique parsing of concatenated strings can be achieved in a variety of different 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[3].

5 General

5.1 Time variant parameters

The mechanisms specified in this document use digital signatures to achieve unilateral or mutual entity authentication. Annex B provides guidance to explain the security properties of the mechanisms and guide users in selecting the appropriate mechanism for their use case.

To prevent valid authentication information from being accepted at a later time, time variant parameters such as time stamps, sequence numbers, or random numbers are used (see ISO/IEC 9798-1:2010, Annex B and the Note below).

If a time stamp or a sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three or four passes (depending on the mechanism employed) are required to achieve mutual authentication.

NOTE The signing by one entity of a data block which has been manipulated by a second entity can be prevented by the first entity including its own random number in the data block which it signs. In this case, it is the unpredictability which prevents the signing of pre-defined data.

5.2 Tokens

Throughout this document, tokens are defined as:

Token = $X_1 \| \cdots \| X_i \| sS_A(Y_1 \| \cdots \| Y_j)$.

In this document, the term "signed data" refers to the data string "$Y_1 \| \cdots \| Y_j$" used as input to the signature scheme and the term "unsigned data" refers to the data string "$X_1 \| \cdots \| X_i$".

Information contained in the unsigned data is, in general, not authenticated by the mechanisms in this document.

If information contained in the signed data of the token can be recovered from the signature [as is the case for signature schemes with message recovery, as specified in ISO/IEC 9796 (all parts)] or is already known to the verifier, then it does not need to be contained in the unsigned data of the token sent by the claimant.

When a signature scheme without message recovery is used, the signed data, M, should be inserted in the unsigned data right before the corresponding signature, i.e. $sS_X(M)$ is replaced by $M \| sS_X(M)$.

Parts of the signed data *M* that are already available to the recipient can be excluded from the unsigned version of *M*.

5.3 Use of text fields

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 C for information on the use of text fields.

6 Requirements

In the authentication mechanisms specified in this document, an entity to be authenticated corroborates its identity by demonstrating its knowledge of its private signature key. This is achieved by the entity using its private signature key to sign specific data. The signature can be verified by anyone using the entity's public verification key.

The authentication mechanisms have the following requirements:

a) A verifier shall possess the valid public key of the claimant, i.e. of the entity that the claimant claims to be.

   One way of obtaining a valid public key is by means of a certificate (see ISO/IEC 9798-1:2010, Annex C). The generation, distribution, and revocation of certificates are outside the scope of this document. Depending on the mechanism, a trusted third party may be used to distribute an authentic copy of the public key and its certificate. Another way of obtaining a valid public key is by a trusted courier.

   As the distribution of certificates is outside the scope of this document, the sending of certificates is optional in all mechanisms.

b) A claimant shall have a private signature key known and used only by the claimant.

c) The private signature key used in an implementation of one of the mechanisms specified in this document shall be distinct from keys used for any other purposes.

d) The data strings signed at various points in an authentication mechanism shall be composed so that they cannot be interchanged.

To help achieve requirement d), the mechanisms in this document include constants SID^i_m in the signed data.

NOTE The form of the constants, SID^i_m, is not specified in this document. However, in order to meet requirement d), 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, the part number, and the authentication mechanism;

— A constant that uniquely identifies the signed string within the mechanism. This constant can be omitted in mechanisms that include only one signed string.

The recipient of a signature shall verify that the constant SID^i_m in the signed data is as expected.

If any of the above requirements is not satisfied, then the authentication process can be compromised or fail to complete successfully.

Annex A defines the object identifiers which shall be used to identify the entity authentication mechanisms specified in this document.

7 Mechanisms without an on-line trusted third party

7.1 Unilateral authentication

7.1.1 General

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

7.1.2 Mechanism UNI.TS — One-pass authentication

In this authentication mechanism, the claimant A initiates the process and is authenticated by the verifier B. Uniqueness and 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 — One-pass unilateral authentication

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

$$\text{Token}AB = \text{Text}2 \| sS_A\left(SID^1_{\text{UNI.TS}} \| \frac{T_A}{N_A} \| i_B \| \text{Text}1 \right),$$

where the claimant, A, uses either a sequence number, N_A, or a time stamp, T_A, as the time variant parameter. The choice depends on the technical capabilities of the claimant and the verifier as well as on the environment.

NOTE 1 The inclusion of the identifier i_B in the signed data of TokenAB is necessary to prevent the token from being accepted by anyone other than the intended verifier.

NOTE 2 One application of this mechanism can be public key or certificate distribution (see ISO/IEC 9798-1:2010, Annex A).

a) A sends TokenAB and, optionally, its identity, I_A, to B.

b) On receipt of the message containing TokenAB, B performs the following steps:

   1) It checks the received identity, I_A, and determines whether this is trusted by verifying the certificate of A, matching it with a stored list of trusted entities or by some other means.

      NOTE 3 It can also check whether the received identity is equal to its own identity. In many applications, authenticating an entity against itself is considered a security issue.

   2) It ensures that it is in possession of a valid public key of A.

   3) It verifies TokenAB by verifying the signature of A contained in the token, by checking the SID, by checking the time stamp or the sequence number, and by checking that the value of the identifier field, (i_B), in the signed data of TokenAB is equal to entity B's distinguishing identifier.

7.1.3 Mechanism UNI.CR — Two-pass authentication

In this authentication mechanism, the claimant, *A*, is authenticated by the verifier, *B*, who initiates the process. Uniqueness and 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.

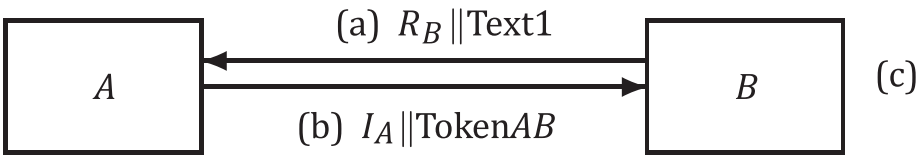

Figure 2 — Two-pass unilateral authentication

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

$$\text{Token}AB = \text{Text3} \parallel sS_A(SID^1_{\text{UNI.CR}} \parallel R_A \parallel R_B \parallel i_B \parallel \text{Text2}).$$

NOTE 1 The inclusion of the identifier, i_B, in the signed data of Token*AB* prevents the token from being accepted by anyone other than the intended verifier (e.g., in a person-in-the-middle attack).

NOTE 2 The inclusion of the random number, R_A, in the signed part of Token*AB* prevents *B* from obtaining the signature of *A* on data chosen by *B* prior to the start of the authentication mechanism.

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

b) *A* sends Token*AB* and, optionally, its identity, I_A, to *B*.

c) On receipt of the message containing Token*AB*, *B* performs the following steps:

1) It checks the received identity, I_A, and determines whether this is trusted either by verifying the certificate of *A*, matching it with a stored list of trusted entities or by some other means.

NOTE 3 It can also check whether the received identity is equal to its own identity. In many applications, authenticating an entity against itself is considered a security issue.

2) It ensures that it is in possession of a valid public key of *A*.

3) It verifies Token*AB* by checking the signature of *A* contained in the token, by checking the *SID*, by checking that the random number, R_B, sent to *A* in step a), agrees with the random number contained in the signed data of Token*AB*, and by checking that the value of the identifier field, (i_B), in the signed data of Token*AB* is equal to *B*'s distinguishing identifier.

7.2 Mutual authentication

7.2.1 General

Mutual authentication means that the two communicating entities are authenticated to each other.

The two mechanisms described in 7.1.2 and 7.1.3 are extended in 7.2.2 and 7.2.3, respectively, to achieve mutual authentication. This is achieved by transmitting one further message resulting in two additional steps.

The mechanism specified in 7.2.4 uses four messages which do not need to be all sent consecutively. In this way, the authentication process can be speeded up.

7.2.2 Mechanism MUT.TS — Two-pass authentication

In this authentication mechanism, uniqueness and 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.

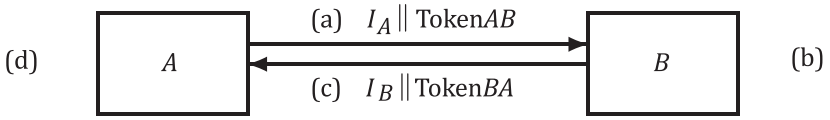

Figure 3 — Two-pass mutual authentication

The form of the token (Token*AB*), sent by *A* to *B*, is analogous to that specified in 7.1.2:

$$\text{Token}AB = \text{Text}2 \| sS_A\left(SID^1_{\text{MUT.TS}} \| \frac{T_A}{N_A} \| i_B \| \text{Text}1 \right).$$

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

$$\text{Token}BA = \text{Text}4 \| sS_B\left(SID^2_{\text{MUT.TS}} \| \frac{T_B}{N_B} \| \frac{T_A}{N_A} \| i_A \| \text{Text}3 \right).$$

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

NOTE 1 The inclusion of identifiers, i_A and i_B, in the signed data of Token*BA* and Token*AB*, respectively, is necessary to prevent the tokens from being accepted by anyone other than the intended verifier.

NOTE 2 If $\frac{T_A}{N_A}$ were to be omitted in Token*BA*, 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 7.1.2 twice. The mechanism no longer achieves mutual authentication.

a) *A* sends Token*AB* and, optionally, its identity, I_A, to *B*.

b) On receipt of the message containing Token*AB*, *B* performs the following steps:

   1) It checks the received identity, I_A, and determines whether this is trusted either by verifying the certificate of *A*, matching it with a stored list of trusted entities or by some other means.

      NOTE 3 It can also check whether the received identity is equal to its own identity. In many applications, authenticating an entity against itself is considered a security issue.

   2) It ensures that it is in possession of a valid public key of *A*.

   3) It verifies Token*AB* by verifying the signature of *A* contained in the token, by checking the *SID*, by checking the time stamp or the sequence number, and by checking that the value of the identifier field, (i_B), in the signed data of Token*AB* is equal to entity *B*'s distinguishing identifier.

c) *B* sends Token*BA* and, optionally, its identity, I_B, to *A*.

d) On receipt of the message containing Token*BA*, *A* performs the following steps:

   1) It checks the received identity, I_B, and determines whether this is trusted either by verifying the certificate of *B*, matching it with a stored list of trusted entities or by some other means.

      NOTE 4 It can also check whether the received identity is equal to its own identity. In many applications, authenticating an entity against itself is considered a security issue.