INTERNATIONAL STANDARD

ISO/IEC 9798-3

Second edition
1998-10-15

AMENDMENT 1
2010-06-01

Information technology — Security techniques — Entity authentication —

Part 3: Mechanisms using digital signature techniques

AMENDMENT 1

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

Partie 3: Mécanismes utilisant des techniques de signature numériques

AMENDEMENT 1

Reference number
ISO/IEC 9798-3:1998/Amd.1:2010(E)

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

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

Published in Switzerland

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 document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Amendment 1 to ISO/IEC 9798-3:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Information technology — Security techniques — Entity authentication —

Part 3:
Mechanisms using digital signature techniques

AMENDMENT 1

Page 1, Clause 3

Replace the first paragraph of Clause 3 with the following:

For the purposes of this part of ISO/IEC 9798, the definitions and notation described in ISO/IEC 9798-1 and the following apply:

I_A The identity of entity *A*, which is either *A* or Cert*A*.

I_B The identity of entity *B*, which is either *B* or Cert*B*.

Res*X* The result of verifying entity *X*'s public key or public key certificate.

Page 5, 5.2.3

Add the following after 5.2.3:

6 Mechanisms involving an on-line trusted third party

6.1 Introduction

The authentication mechanisms in this clause require the two entities *A* and *B* to validate each other's public keys using an on-line trusted third party (with distinguishing identifier *TP*). This trusted third party shall possess reliable copies of the public keys of *A* and *B*. The entities *A* and *B* shall possess a reliable copy of the public key of *TP*.

This clause specifies two five pass authentication mechanisms, both of which achieve mutual authentication between entities *A* and *B*.

In the specification of the two mechanisms, the form of tokens and text fields follow the description given at the beginning of Clause 5, i.e. all paragraphs in Clause 5 before 5.1.

Implementations of the mechanisms shall use one of the signature schemes specified in ISO/IEC 14888 or ISO/IEC 9796.

6.2 Five pass authentication (initiated by *A*)

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

This authentication mechanism is illustrated in Figure 6.

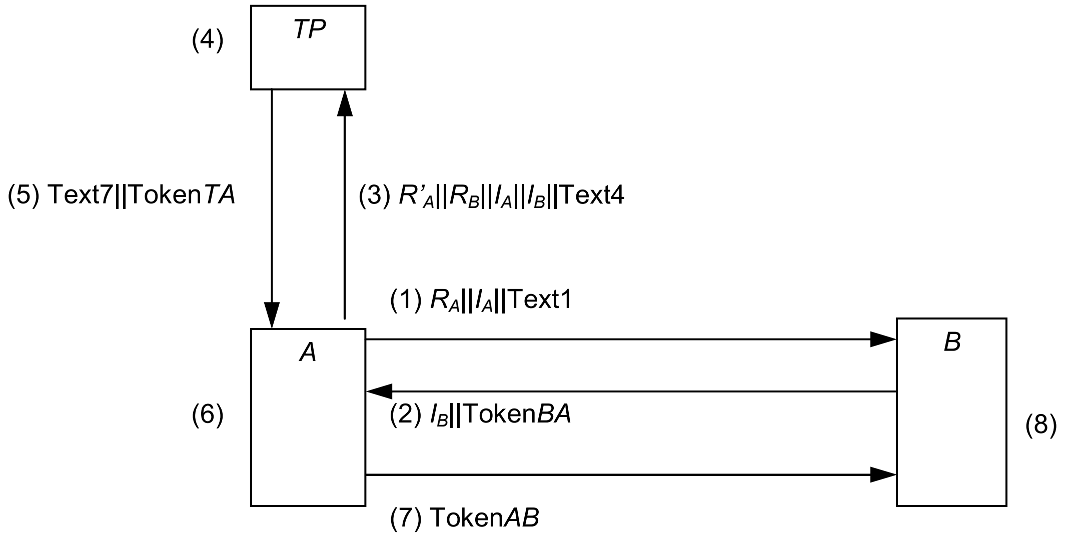

Figure 6 — Five pass authentication (initiated by *A*)

The tokens shall be created according to one of the following two options.

Option 1:

Token*AB* = Text9||Res*A*||$sS_T(R_B||$Res*A*||Text5)||$sS_A(R_B||R_A||B||A||$Text8)

Token*BA* = $R_A||R_B||$Text3||$sS_B(B||R_A||R_B||A||$Text2)

Token*TA* = Res*A*||Res*B*||$sS_T(R'_A||$Res*B*||Text6)||$sS_T(R_B||$Res*A*||Text5)

Option 2:

Token*AB* = R'_A ||Text9||Token*TA*||$sS_A(R_B||R_A||B||A||$Text8)

Token*BA* = $R_A||R_B||$Text3||$sS_B(B||R_A||R_B||A||$Text2)

Token*TA* = Res*A*||Res*B*||$sS_T(R'_A||R_B||$Res*A*||Res*B*||Text5)

The values of the fields I_A, I_B, Res*A*, Res*B*, Status and Failure shall have the following forms:

I_A = *A* or Cert*A*

I_B = *B* or Cert*B*

Res*A* = (Cert*A*||Status), ($A||P_A$) or Failure

Res*B* = (Cert*B*||Status), ($B||P_B$) or Failure

Status = True or False. The value of the field shall be set to False if the certificate is known to have been revoked; otherwise it shall be set to True.

Failure: Res*X* (where $X = \{A, B\}$) will be set to Failure if neither a public key nor a certificate of entity *X* can be found by *TP*.

In the mechanism, if *TP* knows the mapping between identity *X* and P_X (where $X = \{A, B\}$), then it shall set $I_X = X$; otherwise, it shall set I_X = Cert*X*, and *X* shall be set equal to the collection of distinguished identity fields in Cert*X*. If either *X* or Cert*X* is permitted to be used as an identity, then there should be a pre-arranged means to allow *TP* to distinguish the two types of identity indications. The value of Res*X* (where $X = \{A, B\}$) shall be determined according to Table 1.

Table 1 — Value of Res*X*

Field	Choice 1	Choice 2
I_X	*X*	Cert*X*
Res*X*	($X \| P_X$) or Failure	(Cert*X*||Status) or Failure

The mechanism is performed as follows:

1) *A* sends a random number R_A, its identity I_A and, optionally, a text field Text1 to *B*.

2) *B* sends the token Token*BA* and I_B to *A*.

3) *A* sends a random number R'_A, together with R_B, I_A, I_B and, optionally, a text field Text4 to *TP*.

4) On receipt of the message in Step (3) from *A*, *TP* performs the following steps. If $I_A = A$ and $I_B = B$, *TP* retrieves P_A and P_B; If I_A = Cert*A* and I_B = Cert*B*, *TP* checks the validity of Cert*A* and Cert*B*. The process of certificate verification by *TP* may require protection from denial-of-service attacks. The specification of mechanisms to be used to provide such protection is outside of the scope of this part of ISO/IEC 9798.

5) Then *TP* sends Token*TA* and, optionally, a text field Text7 to *A*. The fields Res*A* and Res*B* in Token*TA* shall be: the certificates of *A* and *B* and their status, the distinguishing identifiers of *A* and *B* and their public keys, or an indication of Failure.

6) On receipt of the message in Step (5) from *TP*, *A* performs the following steps:

    (i) Verify Token*TA* by checking the signature of *TP* contained in the token, and by checking that the random number R'_A, sent to *TP* in Step (3), is the same as the random number R'_A contained in the signed data of Token*TA*.

    (ii) Retrieve the public key of *B* from the message, verify Token*BA* received in Step (2) by checking the signature of *B* contained in the token and checking that the value of identifier field (*A*) in the signed data of Token*BA* is equal to *A*'s distinguishing identifier, and then check that the random number R_A, sent to *B* in Step (1), is the same as the random number R_A contained in Token*BA*.

7) *A* sends Token*AB* to *B*.

8) On receipt of the message in Step (7) from *A*, *B* performs the following steps:

    (i) Verify Token*TA* by checking the signature of *TP* contained in the token, and by checking that the random number R_B, sent to *A* in Step (2), is the same as the random number R_B contained in the signed data of Token*TA*.

(ii) Retrieve the public key of A from the message, verify TokenAB by checking the signature of A contained in the token and checking that the value of identifier field (B) in the signed data of TokenAB is equal to B's distinguishing identifier, and then check that the random number R_B contained in the signed data of TokenAB is equal to the random number R_B sent to A in Step (2).

6.3 Five pass authentication (initiated by *B*)

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

This authentication mechanism is illustrated in Figure 7.

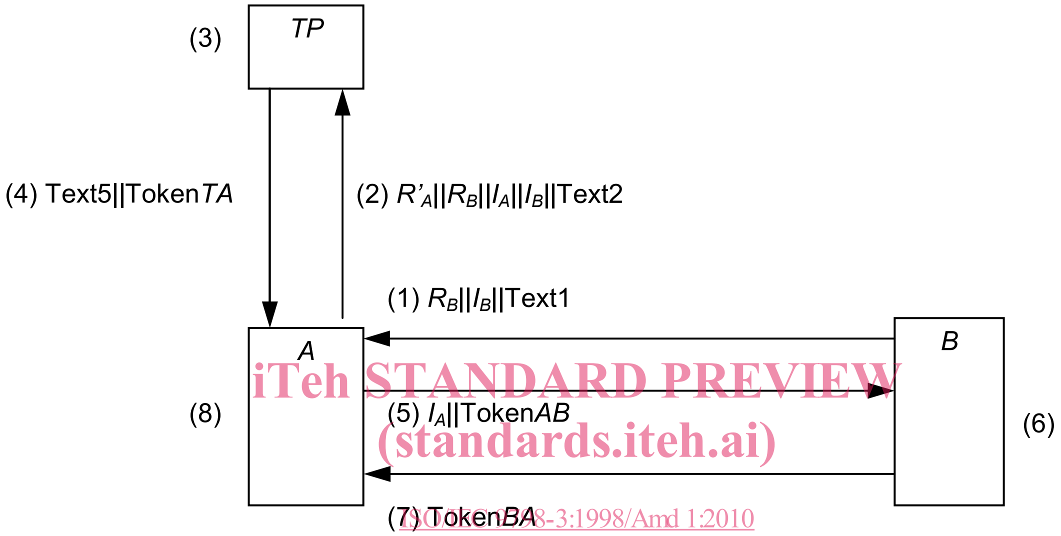

Figure 7 — Five pass authentication (initiated by *B*)

The tokens shall be created according to one of the following two options.

Option 1:

$\text{Token}AB = \text{Text7}\|R_A\|\text{Res}A\|sS_T(R_B\|\text{Res}A\|\text{Text3})\|sS_A(R_B\|R_A\|B\|A\|\text{Text6})$

$\text{Token}BA = R_A\|R_B\|\text{Text9}\|sS_B(A\|R_A\|R_B\|B\|\text{Text8})$

$\text{Token}TA = \text{Res}A\|\text{Res}B\|sS_T(R'_A\|\text{Res}B\|\text{Text4})\|sS_T(R_B\|\text{Res}A\|\text{Text3})$

Option 2:

$\text{Token}AB = R'_A\ \|\text{Text7}\|\text{Token}TA\|sS_A(R_B\|R_A\|B\|A\|\text{Text6})$

$\text{Token}BA = R_A\|R_B\|\text{Text9}\|sS_B(R_A\|R_B\|A\|B\|\text{Text8})$

$\text{Token}TA = \text{Res}A\|\text{Res}B\|sS_T(R'_A\|R_B\|\text{Res}A\|\text{Res}B\|\text{Text3})$

The values of the fields I_A, I_B, Res$A$, Res$B$, Status and Failure shall have the following forms:

$I_A = A$ or Cert$A$

$I_B = B$ or Cert$B$

Res$A$ = (Cert$A$||Status), (A||P_A) or Failure

Res$B$ = (Cert$B$||Status), (B||P_B) or Failure

Status = True or False. The value of the field shall be set to False if the certificate is known to have been revoked; otherwise it shall be set to True.

Failure: Res$Y$ (where $Y = \{A, B\}$) will be set to Failure if neither a public key nor a certificate of entity Y can be found by TP.

In the mechanism, if TP knows the mapping between identity Y and P_Y (where $Y = \{A, B\}$), then it shall set $I_Y = Y$; otherwise, it shall set I_Y = Cert$Y$, and Y shall be set equal to the collection of distinguished identity fields in Cert$Y$. If either Y or Cert$Y$ is permitted to be used as an identity, then there should be a pre-arranged means to allow TP to distinguish the two types of identity indications. The value of Res$Y$ (where $Y = \{A, B\}$) shall be determined according to Table 2.

Table 2 — Value of Res*Y*

Field	Choice 1	Choice 2
I_Y	Y	Cert$Y$
Res$Y$	(Y||P_Y) or Failure	(Cert$Y$||Status) or Failure

The mechanism is performed as follows:

1) B sends a random number R_B, its identity I_B and, optionally, a text field Text1 to A.

2) A sends a random number R'_A, together with R_B, I_A, I_B and, optionally, a text field Text2 to TP.

3) On receipt of the message in Step (2) from A, TP performs the following steps. If $I_A = A$ and $I_B = B$, TP retrieves P_A and P_B; If I_A = Cert$A$ and I_B = Cert$B$, TP checks the validity of Cert$A$ and Cert$B$. The process of certificate verification by TP may require protection from denial-of-service attacks. The specification of mechanisms to be used to provide such protection is outside of the scope of this part of ISO/IEC 9798.

4) Then TP sends TokenTA and, optionally, a text field Text5 to A. The fields Res$A$ and Res$B$ in TokenTA shall be: the certificates of A and B and their status, the distinguishing identifiers of A and B and their public keys or an indication of Failure.

5) A sends the token TokenAB and I_A to B.

6) On receipt of the message in Step (5) from A, B performs the following steps:

   (i) Verify the signature of TP in TokenAB by checking the signature of TP contained in the token, and by checking that the random number R_B, sent to A in Step (1), is the same as the random number R_B contained in the signed data of TP of TokenAB.

   (ii) Retrieve the public key of A from the message, verify TokenAB by checking the signature of A contained in the token and checking that the value of identifier field (B) in the signed data of TokenAB is equal to B's distinguishing identifier, and then check that the random number R_B, sent to A in Step (1), is the same as the random number R_B contained in the signed data of A of TokenAB.

7) B sends TokenBA to A.