

Information technology — Security techniques — Entity authentication —

Part 3: Mechanisms using digital signature techniques

ICS 35.040

National foreword

This British Standard is the UK implementation of ISO/IEC 9798-3:1998+A1:2010, incorporating corrigenda September 2009 and March 2012. It supersedes BS ISO/IEC 9798-3:1998 which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO/IEC text carry the number of the ISO/IEC amendment. For example, text altered by ISO/IEC amendment 1 is indicated by A1 A1.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum September 2009 is indicated in the text by AC1 AC1.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT — Security techniques.

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.

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

Amendments/corrigenda issued since publication

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 December 1998

© The British Standards Institution 2012. Published by BSI Standards Limited 2012.

ISBN 978 0 580 76593 3

Date	Comments
31 July 2010	Implementation of ISO/IEC amendment 1:2010; Implementation of ISO/IEC corrigendum September 2009
30 April 2012	Implementation of ISO/IEC corrigendum March 2012

INTERNATIONAL STANDARD

ISO/IEC
9798-3

Second edition
1998-10-15

Information technology — Security techniques — Entity authentication —

Part 3: Mechanisms using digital signature techniques

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

Partie 3: Mécanismes utilisant des techniques de signature numériques



Contents

	Page
Foreword	iii
1 Scope	1
2 Normative reference	1
3 Definitions and notation	1
4 Requirements	1
5 Mechanisms	2
6 Mechanisms involving an on-line trusted third party	5
Annex A (informative) Use of text fields	10
Bibliography	11
Annex B (normative) Object Identifiers and ASN.1 Syntax	12
Bibliography	14
Figure 1	2
Figure 2	3
Figure 3	3
Figure 4	4
Figure 5	4
Figure 6	5
Figure 7	7

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. 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.

International Standard ISO/IEC 9798-3 was prepared by Joint Technical-Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9798-3:1993), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-3 (1st edition) will be compliant with ISO/IEC 9798-3 (2nd edition).

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

- *Part 1: General*;
- *Part 2: Mechanisms using symmetric encipherment algorithms*;
- *Part 3: Mechanisms using digital signature techniques*;
- *Part 4: Mechanisms using a cryptographic check function*;
- *Part 5: Mechanisms using zero knowledge techniques*.

Further parts may follow.

Annex A of this part of ISO/IEC 9798 is for information only.

Descriptors: Data processing, information interchange, data transmission, protection of information, security techniques, coding (data conversion), authentication, message authentication codes, algorithms.

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using digital signatures based on asymmetric techniques. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities. A digital signature is used to verify the identity of an entity. A trusted third party may be involved.

The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time.

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.

2 Normative reference

The following standard contains provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the edition indicated was valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General*.

3 Definitions and notation

[A1] 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 *CertA*.

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

ResX The result of verifying entity *X*'s public key or public key certificate. **[A1]**

[AC1] As defined in ISO/IEC 9798-1, $X||Y$ is used to mean 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 signed as **[AC1]**

[AC1] part of one of the mechanisms specified in this part of ISO/IEC 9798, 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. This latter property could be achieved in a variety of different ways, depending on the application. For example, it could 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 [1]. **[AC1]**

4 Requirements

In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identity by demonstrating its knowledge of 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.

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

[AC2] c) The private signature key used in an implementation of one of the mechanisms specified in this part of ISO/IEC 9798 shall be distinct from keys used for any other purposes.

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

NOTE This could be enforced by including the following elements in each signed data string:

— The object identifier as specified in Annex B, in particular identifying the ISO standard, the part number, and the authentication mechanism;

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

The recipient of a signature shall verify that the object identifier and the constant identifying the signature position within the mechanism are as expected.

If any of these is not satisfied then the authentication process may be compromised or it cannot be completed successfully. **[AC2]**