AS/NZS ISO/IEC 9798.3:2008
ISO/IEC 9798-3:1998

AS/NZS ISO/IEC 9798.3:2008

Australian/New Zealand Standard™

Information technology—Security techniques—Entity authentication

Part 3: Mechanisms using digital signature techniques

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 25 May 2008 and on behalf of the Council of Standards New Zealand on 31 May 2008.
This Standard was published on 25 June 2008.

The following are represented on Committee IT-012:

Attorney General's Office
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Council of Small Business Organisations
Internet Industry Association
NSW Police
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 07257.

Australian/New Zealand Standard™

Information technology—Security techniques—Entity authentication

Part 3: Mechanisms using digital signature techniques

First published as AS/NZS ISO/IEC 9798.3:2008.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 8770 3

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology.

This Standard is identical with, and has been reproduced from ISO/IEC 9798-3:1998, *Information technology—Security techniques—Entity authentication*—Part 3: *Mechanisms using digital signature techniques*.

The objective of this Standard is to provide the information Security management community with detailed guidance on the background, techniques and procedures of entity authentication mechanisms using digital signature techniques.

This Standard is Part 3 of AS/NZS ISO/IEC 9798, *Information technology—Security techniques—Entity authentication*, which is published in parts as follows:

AS/NZS ISO/IEC	
9798	Information technology—Security techniques—Entity authentication
9798.1	Part 1: General
9798.2	Part 2: Mechanisms using symmetric encipherment algorithms)
9798.3	Part 3: Mechanisms using digital signature techniques (this Standard)
9798.4	Part 4: Mechanisms using a cryptographic check function
9798.5	Part 5: Mechanisms using zero-knowledge techniques
9798.6	Part 6: Mechanisms based on manual data transfer

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text ‘this part of ISO/IEC 9798’ should read ‘this Australian/New Zealand Standard’.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian/New Zealand Standard*	
ISO/IEC		AS/NZS ISO/IEC	
9798	Information technology—Security techniques—Entity authentication	9798	Information technology—Security techniques—Entity authentication
9798-1	Part 1: General	9798.1	Part 1: General

The term ‘informative’ has been used in this Standard to define the application of the annex to which it applies. An ‘informative’ annex is only for information and guidance.

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology — Security techniques — Entity authentication —

Part 3:

Mechanisms using digital signature techniques

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

For the purposes of this part of ISO/IEC 9798 the definitions and notation described in ISO/IEC 9798–1 apply.

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.

If either of these is not satisfied then the authentication process may be compromised or it cannot be completed successfully.

NOTES

1 One way of obtaining a valid public key is by means of a certificate (see Annex C of ISO/IEC 9798-1). The generation, distribution, and revocation of certificates are outside the scope of this part of ISO/IEC 9798. There may exist a trusted third party for this purpose. Another way of obtaining a valid public key is by trusted courier.

2 References to digital signature schemes are contained in Annex D of ISO/IEC 9798-1.