

Australian/New Zealand Standard™

**Information technology—Security  
techniques—Entity authentication**

**Part 4: Mechanisms using a  
cryptographic check function**



## **AS/NZS ISO/IEC 9798.4:2008**

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 28 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

Additional Interests:

Fujitsu

---

### **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 Standards may also be withdrawn.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](http://www.standards.com.au) or Standards New Zealand web site at [www.standards.co.nz](http://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 07256.*

---

Australian/New Zealand Standard™

**Information technology—Security  
techniques—Entity authentication**

**Part 4: Mechanisms using a  
cryptographic check function**

First published as AS/NZS ISO/IEC 9798.4:2008.

**COPYRIGHT**

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

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

ISBN 0 7337 8771 1

## 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 9798-4:1999, *Information technology—Security techniques—Entity authentication, Part 4: Mechanisms using a cryptographic check function*.

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 a cryptographic check function.

This Standard is Part 4 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
9798.4	Part 4: Mechanisms using a cryptographic check function (this Standard)
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:

- Its number appears on the cover and title page while the international standard number appears only on the cover.
- In the source text ‘this part of ISO/IEC 9798’ should read ‘this Australian/New Zealand Standard’.
- 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:

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

Only international references that have been adopted as Australian or Australian/New Zealand Standards have been listed.

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.

## CONTENTS

	<i>Page</i>
<b>1</b>	<b>Scope .....</b> 1
<b>2</b>	<b>Normative references.....</b> 1
<b>3</b>	<b>Definitions and notation .....</b> 1
<b>4</b>	<b>Requirements.....</b> 1
<b>5</b>	<b>Mechanisms .....</b> 2
<b>5.1</b>	<b>Unilateral authentication.....</b> 2
<b>5.1.1</b>	<b>One pass authentication.....</b> 2
<b>5.1.2</b>	<b>Two pass authentication.....</b> 3
<b>5.2</b>	<b>Mutual authentication .....</b> 4
<b>5.2.1</b>	<b>Two pass authentication.....</b> 4
<b>5.2.2</b>	<b>Three pass authentication.....</b> 5
<b>Annex A</b>	<b>Use of text fields.....</b> 7

## AUSTRALIAN/NEW ZEALAND STANDARD

# Information technology—Security techniques—Entity authentication

## Part 4: Mechanisms using a cryptographic check function

### 1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using a cryptographic check function. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities.

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 or more than once.

If 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 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.

Examples of cryptographic check functions are given in ISO/IEC 9797.

### 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*.

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 a secret authentication key. This is achieved by the entity using its secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. The cryptographic check value can be checked by anyone sharing the entity's secret authentication key, who can recalculate the cryptographic check value and compare it with the value received.