Australian Standard™

Information technology—Security techniques—Entity authentication

Part 5: Mechanisms using zero-knowledge techniques

This Australian Standard was prepared by Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 31 March 2006.
This Standard was published on 1 May 2006.

The following are represented on Committee IT-012:

Attorney General's Department
Australia Post
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Australian Information Industry Association
Certification Forum of Australia
Consumers' Federation of Australia
Department of Defence (Australia)
Department of Social Welfare New Zealand
Government Communications Security Bureau, New Zealand
Internet Industry Association
NSW Police Service
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 Standards may also be withdrawn.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 Standards can be found by visiting the Standards Web Shop at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to the Chief Executive, Standards Australia, GPO Box 476, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 06034.

Australian Standard™

Information technology—Security techniques—Entity authentication

Part 5: Mechanisms using zero-knowledge techniques

First published as AS ISO/IEC 9798.5—2006.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 7386 9

PREFACE

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

After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian Standard rather than an Australian/New Zealand Standard.

This Standard is identical with, and has been reproduced from ISO/IEC 9798-5:2004, *Information technology—Security techniques—Entity authentication—Part 5: Mechanisms using zero-knowledge 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 zero-knowledge techniques.

This Standard is Part 5 of AS 9798, *Information technology—Security techniques—Entity authentication*, which, when complete, will consist of the following:

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 (this standard)
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 International Standard' should read 'this Australian Standard'.

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

The terms 'normative' and 'informative' are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

CONTENTS

Page

NOTES

AUSTRALIAN STANDARD

Information technology — Security techniques — Entity authentication —

Part 5:
Mechanisms using zero-knowledge techniques

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using zero-knowledge techniques.

— Clause 5 specifies mechanisms (already present in the first edition, ISO/IEC 9798-4:1999) based on identities and providing unilateral authentication. They have been repaired after the withdrawal of ISO/IEC 9796:1991.

— Clause 6 specifies mechanisms (inserted in this second edition) based on integer factorization and providing unilateral authentication.

— Clauses 7 and 8 specify mechanisms based on discrete logarithms with respect to numbers that are either prime (see Clause 7, mechanisms already present in the first edition) or composite (see Clause 8, mechanisms inserted in the second edition), and providing unilateral authentication.

— Clause 9 specifies mechanisms based on asymmetric encipherment systems and providing either unilateral (see 9.3, mechanisms already present in the first edition), or mutual (see 9.4, mechanisms inserted in the second edition) authentication.

The verifier associates the correct verification key with the claimant by any appropriate procedure, for example, by retrieving it from a certificate. Such procedures are outside the scope of this part of ISO/IEC 9798.

To identify each mechanism, Annex A specifies object identifiers in accordance with ISO/IEC 8825-1.

These mechanisms are constructed using the principles of zero-knowledge techniques, but they will not be zero-knowledge according to the strict definition sketched in Annex B for every choice of parameters.

Annex C compares the mechanisms and provides guidance on parameter choices.

Annex D provides numerical examples.

2 Normative references

The following referenced documents are indispensable for the application 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 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*