AS/NZS ISO/IEC 11770.2:2008
ISO/IEC 11770-2:1996
ISO/IEC 11770-2:1996/Cor.1:2005

AS/NZS ISO/IEC 11770.2:2008

Australian/New Zealand Standard™

Information technology—Security techniques—Key management

Part 2: Mechanisms using symmetric 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 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

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 Standards may also be withdrawn.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 07259.

Australian/New Zealand Standard™

Information technology—Security techniques—Key management

Part 2: Mechanisms using symmetric techniques

First published as AS/NZS ISO/IEC 11770.2:2008.

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 8764 9

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 11770-2:1996, *Information technology—Security techniques—Key management,* Part 2: *Mechanisms using symmetric techniques* and its corrigendum ISO/IEC 11770.2:1996/Cor.1:2005 which is added to the end of the source text.

The objective of this Standard is to provide the information security management community with detailed guidance on key establishment mechanisms using symmetric cryptographic techniques.

This Standard is Part 2 of AS 11770, *Information technology—Security techniques—Key management*, which is published in parts as follows:

AS/NZS		
11770	Information technology—Security techniques—Key management	
11770.1	Part 1:	Framework
11770.2	Part 2:	Mechanisms using symmetric techniques (this Standard)
11770.3	Part 3:	Mechanisms using asymmetric techniques
11770.4	Part 4:	Mechanisms based on weak secrets

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 11770’ 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	
9798	Information technology—Security techniques—Entity authentication	9798	Information technology—Security techniques—Entity authentication
9798-2	Part 2: Mechanisms using symmetric encipherment algorithms	9798.2	Part 2: Mechanisms using symmetric encipherment algorithms
9798-4	Part 4: Mechanisms using a cryptographic check function	9798.4	Part 4: Mechanisms using a cryptographic check function
11770	Information technology—Security techniques—Key management		
11770-1	Part 1: Framework	AS/NZS ISO/IEC	
		11770	Information technology—Security techniques—Key management
		11770.1	Part 1: Framework

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.

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology — Security techniques — Key management —

Part 2:
Mechanisms using symmetric techniques

1 Scope

The purpose of key management is to provide procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic algorithms according to the security policy in force. This part of ISO/IEC 11770 defines key establishment mechanisms using symmetric cryptographic techniques.

Key establishment mechanisms using symmetric cryptographic techniques can be derived from entity authentication mechanisms of ISO/IEC 9798-2 and ISO/IEC 9798-4 by specifying the use of text fields available in those mechanisms. Other key establishment mechanisms exist for specific environments; see for example ISO 8732. Besides key establishment, goals of such a mechanism may include unilateral or mutual authentication of the communicating entities. Further goals may be the verification of the integrity of the established key, or key confirmation.

This part of ISO/IEC 11770 addresses three environments for the establishment of keys: Point-to-Point, Key Distribution Centre (KDC) and Key Translation Centre (KTC). This part of ISO/IEC 11770 describes the required content of messages which carry keying material or are necessary to set up the conditions under which the keying material can be established. The document does not indicate other information which may be contained in the messages or specify other messages such as error messages. The explicit format of messages is not within the scope of this part of ISO/IEC 11770.

This part of ISO/IEC 11770 does not explicitly address the issue of interdomain key management. This part of ISO/IEC 11770 also does not define the implementation of key management mechanisms; there may be different products that comply with this part of ISO/IEC 11770 and yet are not compatible.

1 To be published.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 11770. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 11770 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2: 1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

ISO/IEC 9798-2: 1994, *Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms.*

ISO/IEC 9798-4: 1995, *Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function.*

ISO/IEC 11770-1: - [1], *Information technology - Security techniques - Key management - Part 1: Key management framework.*

3 Definitions and Notation

3.1 Definitions

For the purposes of this part of ISO/IEC 11770 the definitions given in ISO/IEC 11770-1 apply. In addition, this part of ISO/IEC 11770 makes use of the following terms:

3.1.1 distinguishing identifier: Information which unambiguously distinguishes an entity.

COPYRIGHT