AS/NZS ISO/IEC 11770.4:2008
ISO/IEC 11770-4:2006

AS/NZS ISO/IEC 11770.4:2008

Australian/New Zealand Standard™

Information technology—Security techniques—Key management

Part 4: Mechanisms based on weak secrets

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 19 February 2007 and on behalf of the Council of Standards New Zealand on 21 September 2007.
This Standard was published on 5 February 2008.

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, NZ
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 Standards may also be withdrawn.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 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 06487.

Australian/New Zealand Standard™

Information technology—Security techniques—Key management

Part 4: Mechanisms based on weak secrets

First published as AS/NZS ISO/IEC 11770.4:2008.

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

ISBN 0 7337 8411 9

PREFACE

This Standard was prepared by the Australian members of 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 11770-4:2006, *Information technology—Security techniques—Key management,* Part 4: *Mechanisms based on weak secrets*.

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.

This Standard is Part 4 of AS 11770, *Information technology—Security techniques—Key management*, which is published in parts as follows:

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

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 ISO/IEC	
10118	Information technology—Security techniques—Hash-functions	10118	Information technology—Security techniques—Hash-functions
10118-3	Part 3: Dedicated hash-functions	10118.3	Part 3: Dedicated hash-functions
		AS/NZS ISO/IEC	
11770	Information technology—Security techniques—Key management	11770	Information technology—Security techniques—Key management
11770-1	Part 1: Framework	11770.1	Part 1: Framework

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

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology—Security techniques—Key management

Part 4: Mechanisms based on weak secrets

1 Scope

This part of ISO/IEC 11770 defines key establishment mechanisms based on weak secrets, i.e., secrets that can be readily memorized by a human, and hence secrets that will be chosen from a relatively small set of possibilities. It specifies cryptographic techniques specifically designed to establish one or more secret keys based on a weak secret derived from a memorized password, while preventing off-line brute-force attacks associated with the weak secret. More specifically, these mechanisms are designed to achieve one of the following three goals.

1) **Balanced password-authenticated key agreement:** Establish one or more shared secret keys between two entities that share a common weak secret. In a balanced password-authenticated key agreement mechanism, the shared secret keys are the result of a data exchange between the two entities, the shared secret keys are established if and only if the two entities have used the same weak secret, and neither of the two entities can predetermine the values of the shared secret keys.

2) **Augmented password-authenticated key agreement:** Establish one or more shared secret keys between two entities *A* and *B*, where *A* has a weak secret and *B* has verification data derived from a one-way function of *A*'s weak secret. In an augmented password-authenticated key agreement mechanism, the shared secret keys are the result of a data exchange between the two entities, the shared secret keys are established if and only if the two entities have used the weak secret and the corresponding verification data, and neither of the two entities can predetermine the values of the shared secret keys.

   NOTE – This type of key agreement mechanism is unable to protect *A*'s weak secret being discovered by *B*, but only increases the cost for an adversary to get *A*'s weak secret from *B*. Therefore it is normally used between a client (*A*) and a server (*B*).

3) **Password-authenticated key retrieval:** Establish one or more secret keys for an entity, *A*, associated with another entity, *B*, where *A* has a weak secret and *B* has a strong secret associated with *A*'s weak secret. In an authenticated key retrieval mechanism, the secret keys, retrievable by *A* (not necessarily derivable by *B*), are the result of a data exchange between the two entities, and the secret keys are established if and only if the two entities have used the weak secret and the associated strong secret. However, although *B*'s strong secret is associated with *A*'s weak secret, the strong secret does not (in itself) contain sufficient information to permit either the weak secret or the secret keys established in the mechanism to be determined.

   NOTE – This type of key retrieval mechanism is used in those applications where *A* does not have secure storage for a strong secret, and requires *B*'s assistance to retrieve the strong secret for her. It is normally used between a client (*A*) and a server (*B*).

This part of ISO/IEC 11770 does not cover aspects of key management such as

— lifecycle management of weak secrets, strong secrets and established secret keys;

— mechanisms to store, archive, delete, destroy, etc. weak secrets, strong secrets, and established secret keys.