AS/NZS ISO/IEC 11770.3:2008
ISO/IEC 11770-3:1999

AS/NZS ISO/IEC 11770.3:2008

Australian/New Zealand Standard™

Information technology—Security techniques—Key management

Part 3: Mechanisms using asymmetric 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 Standards may also be withdrawn.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 07104.

Australian/New Zealand Standard™

Information technology—Security techniques—Key management

Part 3: Mechanisms using asymmetric techniques

First published as AS/NZS ISO/IEC 11770.3:2008.

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

ISBN 0 7337 8766 5

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 11770-3:1999, *Information technology—Security techniques—Key management,* Part 3: *Mechanisms using asymmetric 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.

This Standard is Part 3 of AS/NZS ISO/IEC 11770, *Information technology—Security techniques—Key management*, which is published in parts as follows:

Part 1: Framework
Part 2: Mechanisms using symmetric techniques
Part 3: Mechanisms using asymmetric techniques (this Standard)
Part 4: Mechanisms based on weak secrets

The term 'informative' is used to define the application of the annex to which it applies. An informative annex is only for information and guidance.

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
9798-3	Part 3: Mechanisms using digital signature techniques	9798.3	Part 3: Mechanisms using digital signature techniques
9594-8	Information technology—Open Systems Interconnection—The Directory: Public-key and attribute certificate frameworks—Part 8	4019 4019.8	Information technology—Open Systems Interconnection—The Directory: Authentication framework Part 8: Authentication framework
		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: Key management framework
		AS ISO/IEC	
10118	Information technology—Security techniques—Hash-functions	10118	Information technology—Security techniques—Hash-functions
10118-1	Part 1: General	10118.1	Part 1: General

ISO		AS	
7498	Information processing systems—Open Systems Interconnection—Basic Reference Model	2772	Information processing systems—Open Systems Interconnection—Basic Reference Model
7498-2	Part 2: Security Architecture	2772.2	Part 2: Security Architecture

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

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology—Security techniques—Key management

Part 3:
Mechanisms using asymmetric techniques

1. Scope

This part of ISO/IEC 11770 defines key management mechanisms based on asymmetric cryptographic techniques. It specifically addresses the use of asymmetric techniques to achieve the following goals:

1. Establish a shared secret key for a symmetric cryptographic technique between two entities *A* and *B* by key agreement. In a secret key agreement mechanism the secret key is the result of a data exchange between the two entities *A* and *B*. Neither of them can predetermine the value of the shared secret key.
2. Establish a shared secret key for a symmetric cryptographic technique between two entities *A* and *B* by key transport. In a secret key transport mechanism the secret key is chosen by one entity *A* and is transferred to another entity *B*, suitably protected by asymmetric techniques.
3. Make an entity's public key available to other entities by key transport. In a public key transport mechanism, the public key of an entity A must be transferred to other entities in an authenticated way, but not requiring secrecy.

Some of the mechanisms of this part of ISO/IEC 11770 are based on the corresponding authentication mechanisms in ISO/IEC 9798-3.

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

- key lifecycle management,
- mechanisms to generate or validate asymmetric key pairs,
- mechanisms to store, archive, delete, destroy, etc. keys.

While this part of ISO/IEC 11770 does not explicitly cover the distribution of an entity's private key (of an asymmetric key pair) from a trusted third party to a requesting entity, the key transport mechanisms described can be used to achieve this.

This part of ISO/IEC 11770 does not cover the implementations of the transformations used in the key management mechanisms.

NOTE - To achieve authenticity of key management messages it is possible to make provisions for authenticity within the key establishment protocol or to use a public key signature system to sign the key exchange messages.

2. Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 11770. 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 11770 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.