

Australian Standard™

**Information technology—Security
techniques—Key management**

Part 1: Framework

This Australian Standard was prepared by Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 4 March 2003 and published on 31 March 2003.

The following are represented on Committee IT-012:

Attorney General's Department
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
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 Standards may also be withdrawn.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 Australia web site 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 Australian Standard*, has a full listing of revisions and amendments published each month.

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.com.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

Australian Standard™

**Information technology—Security
techniques—Key management**

Part 1: Framework

First published as AS 11770.1—2003.

COPYRIGHT

© Standards Australia International

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.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5118 0

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

This Standard is identical with, and has been reproduced, from ISO/IEC 11770-1:1996, *Information technology—Security techniques—Key management, Part 1: Framework*.

The objective of this Standard is to define the basic concepts, services and characteristics of the mechanisms of key management while describing specific requirements and a framework for the management of keying material during its life cycle.

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.

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 11770-1’ should read ‘this Australian 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:

<i>Reference to International Standard</i>		<i>Australian Standard</i>	
ISO		AS	
7498	Information processing systems— Open Systems Interconnection—Basic reference model	2777	Information processing systems— Open Systems Interconnection—Basic reference model
7498-2	Part 2: Security architecture	2777.2	Part 2: Security architecture

CONTENTS

Page

1 Scope	1
2 Normative References	1
3 Definitions	1
4 General Discussion of Key Management	2
4.1 Protection of Keys	3
4.1.1 Protection by Cryptographic Techniques	3
4.1.2 Protection by non-Cryptographic Techniques	3
4.1.3 Protection by Physical Means	3
4.1.4 Protection by Organisational Means	3
4.2 Generic Key Life Cycle Model	3
4.2.1 Transitions between Key States	4
4.2.2 Transitions, Services and Keys	4
5 Concepts of Key Management	5
5.1 Key Management Services	5
5.1.1 Generate-Key	6
5.1.2 Register-Key	6
5.1.3 Create-Key-Certificate	6
5.1.4 Distribute-Key	6
5.1.5 Install-Key	6
5.1.6 Store-Key	6
5.1.7 Derive-Key	7
5.1.8 Archive-Key	7
5.1.9 Revoke-Key	7
5.1.10 Deregister-Key	7
5.1.11 Destroy-Key	7
5.2 Support Services	7
5.2.1 Key Management Facility Services	7
5.2.2 User-oriented Services	7
6 Conceptual Models for Key Distribution	8
6.1 Key Distribution between Communicating Entities	8
6.2 Key Distribution within One Domain	8
6.3 Key Distribution between Domains	9
7 Specific Service Providers	10

Annexes

A Threats to Key Management	11
B Key Management Information Objects	12
C Classes of Cryptographic Applications	14
C.1 Authentication Services and Keys.....	14
C.2 Encipherment Services and Keys	15
D Certificate Lifecycle Management	16
D.1 The Certification Authority.....	16
D.1.1 The CA's Asymmetric Key Pair	16
D.2 The Certification Process.....	16
D.2.1 Model for Public Key Certification	16
D.2.2 Registration	18
D.2.3 Relationships between Legal Entities.....	18
D.2.4 Certificate Generation	18
D.2.5 Renewal/Lifetime	18
D.3 Distribution and Use of Public Key Certificates.....	19
D.3.1 Distribution and Storage of Public Key Certificates.....	19
D.3.2 Verification of Public Key Certificates.....	19
D.4 Certification Paths.....	19
D.5 Certificate Revocation.....	19
D.5.1 Revocation Lists	19
E Bibliography	21

AUSTRALIAN STANDARD

Information technology — Security techniques — Key management —

Part 1: Framework

1 Scope

This part of ISO/IEC 11770:

1. identifies the objective of key management;
2. describes a general model on which key management mechanisms are based;
3. defines the basic concepts of key management common to all the parts of this multi-part standard;
4. defines key management services;
5. identifies the characteristics of key management mechanisms;
6. specifies requirements for the management of keying material during its life cycle; and
7. describes a framework for the management of keying material during its life cycle.

This framework defines a general model of key management that is independent of the use of any particular cryptographic algorithm. However, certain key distribution mechanisms may depend on particular algorithm properties, for example, properties of asymmetric algorithms.

Specific key management mechanisms are addressed by other parts of ISO/IEC 11770. Symmetric mechanisms are addressed in part 2 (ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*). Asymmetric mechanisms are addressed in part 3 (ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*). This part of ISO/IEC 11770 contains the material required for a basic understanding of parts 2 and 3. Examples of the use of key management mechanisms are included in ISO 8732 and ISO 11166. If non-repudiation is required for key management, ISO/IEC 13888 should be used.

This part of ISO/IEC 11770 addresses both the automated and manual aspects of key management, including outlines of data elements and sequences of operations that are used to obtain key management services. However it does not specify details of protocol exchanges that may be needed.

As with other security services, key management can only be provided within the context of a defined security policy. The definition of security policies is outside the scope of this multi-part standard.

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 edition 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 9798-1: 1991, *Information technology — Security techniques — Entity authentication mechanisms — Part 1: General model*.

ISO/IEC 10181-1: 1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*.

3 Definitions

The following terms are used as defined in ISO 7498-2:

data integrity

data origin authentication

digital signature

The following term is used as defined in ISO/IEC 9798-1:

entity authentication

The following terms are used as defined in ISO/IEC 10181-1:

security authority

security domain

trusted third party (TTP)