

Australian Standard™

**Information technology—Security  
techniques—Specification of TTP  
services to support the application of  
digital signatures**

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 29 January 2004 and published on 17 March 2004.

---

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 Standards may also be withdrawn.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 Web Shop at [www.standards.com.au](http://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](mailto:mail@standards.org.au), or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

---

*This Standard was issued in draft form for comment as DR 03546.*

Australian Standard™

**Information technology—Security  
techniques—Specification of TTP  
services to support the application of  
digital signatures**

First published as AS 5045—2004.

**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 5762 6

## 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 15945:2002, *Information technology—Security techniques—Specification of TTP services to support the application of digital signatures*.

The objective of this Standard is to define those TTP services needed to support the application of digital signatures for the purpose of non-repudiation of creation of documents. It also defines interfaces and protocols to enable interoperability between entities associated with these TTP services.

As this Standard is reproduced from an international standard, the following applies:

- its number appears on the cover and title page while the international standard number appears only on the cover
- In the source text ‘this International Standard’ should read ‘this Australian Standard’.
- 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/IEC	AS
11770-1 Information technology—Security techniques—Key management—Part 1: Framework	11770.1 Information technology—Security techniques—Key management, Part 1: Framework

## CONTENTS

Page

1	Scope .....	1
2	Normative references .....	1
	2.1 Identical Recommendations   International Standards .....	2
	2.2 Additional references .....	2
3	Definitions .....	3
4	Abbreviations .....	4
5	Descriptive classification of services .....	5
	5.1 Certificate management services .....	5
	5.2 Key management services .....	8
	5.3 Other services .....	9
6	Minimal certificate and CRL profile .....	10
	6.1 Minimal certificate profile .....	10
	6.2 Minimal CRL profile .....	11
7	Certificate management messages .....	11
	7.1 Overview of certificate management services and messages .....	12
	7.2 Assumptions and restrictions for some of the services .....	15
8	Data structures for certificate management messages .....	19
	8.1 Overall message .....	19
	8.2 Common Data Structures .....	22
	8.3 Data structures specific for Certificate Request Messages of type CertReq .....	24
	8.4 Data structures specific for other messages .....	29
	8.5 Transport protocols .....	32
	8.6 Complete ASN.1 Module .....	32
9	Online Certificate Status Protocol .....	40
	9.1 Protocol Overview .....	40
	9.2 Functional Requirements .....	42
	9.3 Detailed Protocol .....	43
	9.4 ASN.1 Module for OCSP .....	47
	Annex A – Interworking .....	50
	Annex B – Algorithms .....	51
	B.1 Hash Algorithms .....	51
	B.2 Digital Signature Algorithms .....	51
	Annex C – Bibliography .....	52

NOTES

## AUSTRALIAN STANDARD

# INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – SPECIFICATION OF TTP SERVICES TO SUPPORT THE APPLICATION OF DIGITAL SIGNATURES

## 1 Scope

This Recommendation | International Standard will define those TTP services needed to support the application of digital signatures for the purpose of non-repudiation of creation of documents.

This Recommendation | International Standard will also define interfaces and protocols to enable interoperability between entities associated with these TTP services.

Definitions of technical services and protocols are required to allow for the implementation of TTP services and related commercial applications.

This Recommendation | International Standard focuses on:

- implementation and interoperability;
- service specifications; and
- technical requirements.

This Recommendation | International Standard does not describe the management of TTPs or other organizational, operational or personal issues. Those topics are mainly covered in ITU-T Rec. X.842 | ISO/IEC TR 14516, *Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services*.

NOTE 1 – Because interoperability is the main issue of this Recommendation | International Standard, the following restrictions hold:

- i) Only those services which may be offered by a TTP, either to end entities or to another TTP, are covered in this Recommendation | International Standard.
- ii) Only those services which may be requested and/or delivered by means of standardizable digital messages are covered.
- iii) Only those services for which widely acceptable standardized messages can be agreed upon at the time this Recommendation | International Standard is published are specified in detail.

Further services will be specified in separate documents when widely acceptable standardized messages are available for them. In particular, time stamping services will be defined in a separate document.

NOTE 2 – The data structures and messages in this Recommendation | International Standard will be specified in accordance to RFC documents, RFC 2510 and RFC 2511 (for certificate management services) and to RFC 2560 (for OCSP services). The certificate request format also allows interoperability with PKCS#10. See Annex C for references to the documents mentioned in this Note.

NOTE 3 – Other standardization efforts for TTP services in specific environments and applications, like SET or EDIFACT, exist. These are outside of the scope of this Recommendation | International Standard.

NOTE 4 – This Recommendation | International Standard defines technical specifications for services. These specifications are independent of policies, specific legal regulations, and organizational models (which, for example, might define how duties and responsibilities are shared between Certification Authorities and Registration Authorities). Of course, the policy of TTPs offering the services described in this Recommendation | International Standard will need to specify how legal regulations and the other aspects mentioned before will be fulfilled by the TTP. In particular, the policy has to specify how the validity of digital signatures and certificates is determined.

## 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this Recommendation | International Standard 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. The Telecommunication Standardization Bureau of ITU maintains a list of currently valid ITU-T Recommendations.