

Australian/New Zealand Standard™

**Information technology—Security  
techniques—Security requirements for  
cryptographic modules**



## **AS/NZS ISO/IEC 19790:2006**

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 23 June 2006 and on behalf of the Council of Standards New Zealand on 30 June 2006. This Standard was published on 26 July 2006.

---

The following are represented on Committee IT-012:

Attorney General's Department  
Australian Association of Permanent Building Societies  
Australian Bankers Association  
Australian Chamber Commerce and Industry  
Australian Electrical and Electronic Manufacturers Association  
Certification Forum of Australia  
Department of Defence  
Department of Social Welfare, NZ  
Government Communications Security Bureau, NZ  
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 Standards may also be withdrawn.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 joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at [www.standards.com.au](http://www.standards.com.au) or Standards New Zealand web site at [www.standards.co.nz](http://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 06207.*

---

Australian/New Zealand Standard™

**Information technology—Security techniques—Security requirements for cryptographic modules**

First published as AS/NZS ISO/IEC 19790:2006.

**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 7620 5