Australian Standard®

# Information technology—Security techniques—Hash-functions

## Part 3: Dedicated hash-functions



This Australian Standard® was prepared by Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 23 June 2006.
This Standard was published on 2 August 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

---

This Standard was issued in draft form for comment as DR 06302.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through public comment period.

---

## Keeping Standards up-to-date

Australian Standards® are living documents that 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Standards may also be withdrawn.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 that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

---

Australian Standard®

# Information technology—Security techniques—Hash-functions

# Part 3: Dedicated hash-functions

First published as AS ISO/IEC 10118.3—2006.



Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 7665 5

# PREFACE

This Standard was prepared by the Standards Australia Committee IT-012, Information Systems, Security and Identification.

The objective of this Standard is to specify dedicated hash-functions, i.e. specifically designed hash-functions. The hash-functions in this Standard are based on the iterative use of round-function. Seven distinct round-functions are specified, giving rise to distinct dedicated hash-functions.

This Standard is identical with, and has been reproduced from ISO/IEC 10118-3:2004, *Information technology—Security techniques—Hash-functions*—Part 3: *Dedicated hash-functions*.

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 10118' 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:

| *Reference to International Standard* | | *Australian Standard* | |
|---|---|---|---|
| ISO/IEC | | 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 |

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*

NOTES

AUSTRALIAN STANDARD

# Information technology — Security techniques — Hash-functions —

# Part 3:
# Dedicated hash-functions

## 1 Scope

This part of ISO/IEC 10118 specifies dedicated hash-functions, i.e. specially designed hash-functions. The hash-functions in this part of ISO/IEC 10118 are based on the iterative use of a round-function. Seven distinct round-functions are specified, giving rise to distinct dedicated hash-functions.

The first and third dedicated hash-functions in Clauses 7 and 9 respectively provide hash-codes of lengths up to 160 bits; the second in Clause 8 provides hash-codes of lengths up to 128 bits; the fourth in Clause 10 provides hash-codes of lengths up to 256 bits; the sixth in Clause 12 provides hash-codes of a fixed length, 384 bits; and the fifth and seventh in Clauses 11 and 13 respectively provide hash-codes of lengths up to 512 bits.

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10118-1:2000, *Information technology — Security techniques — Hash-functions — Part 1: General*

## 3 Terms and definitions

For the purposes of this part of ISO/IEC 10118, the definitions given in ISO/IEC 10118-1 and the following apply.

**3.1**
**block**
a bit-string of length $l$, i.e. the length of the first input to the round-function

**3.2**
**word**
a string of 32 bits used in dedicated hash-functions 1, 2, 3 and 4 of Clauses 7, 8, 9 and 10 respectively, or a string of 64 bits used in dedicated hash-functions 5 and 6 of Clauses 11 and 12 respectively

**3.3**
**matrix**
an $n$ by 8 matrix in which each entry is a string of 8 bits used in dedicated hash-function 7 of Clause 13

## 4 Symbols (and abbreviated terms)

### 4.1 Symbols specified in ISO/IEC 10118-1

This part of ISO/IEC 10118 makes use of the following symbols and notations defined in ISO/IEC 10118-1.

$B_i$ A byte.