Australian Standard®

# Information technology—Security techniques—Hash-functions

## Part 1: General



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 06299.

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Standards may also be withdrawn.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 1: General

First published as AS ISO/IEC 10118.1—2006.



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

ISBN 0 7337 7663 9

# PREFACE

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

The objective of this Standard to specify hash-functions and is therefore applicable to the provision of authentication, integrity and non-repudiation services. Hash-functions map arbitrary strings of bits to a fixed-length strings of bits, using a specified algorithm. They can be used for reducing a message to a short imprint for input to a digital signature mechanism, and committing the user to a given string of bits without revealing this string.

This Standard is identical with, and has been reproduced from ISO/IEC 10118-1:2000, *Information technology—Security techniques—Hash-functions*—Part 1: *General*.

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.

The term 'normative' has been used in this Standard to define the application of the annex to which it applies. A 'normative' annex is an integral part of a Standard.

AUSTRALIAN STANDARD

# Information technology — Security techniques — Hash-functions —

# Part 1:
# General

## 1 Scope

ISO/IEC 10118 specifies hash-functions and is therefore applicable to the provision of authentication, integrity and non-repudiation services. Hash-functions map arbitrary strings of bits to a fixed-length strings of bits, using a specified algorithm. They can be used for

- reducing a message to a short imprint for input to a digital signature mechanism, and

- committing the user to a given string of bits without revealing this string.

NOTE - The hash-functions specified in this part of ISO/IEC 10118 do not involve the use of secret keys. However, these hash-functions may be used, in conjunction with secret keys, to build message authentication codes. Message Authentication Codes (MACs) provide data origin authentication as well as message integrity. For the calculation of a MAC the user is referred to ISO/IEC 9797.

This part of ISO/IEC 10118 contains definitions, symbols, abbreviations and requirements, that are common to all the other parts of ISO/IEC 10118.

## 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10118. 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/IEC 10118 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.

ISO/IEC 9797 (all parts), *Information technology – Security techniques – Message Authentication Codes (MACs).*

## 3 Terms and definitions

For the purposes of this part of ISO/IEC 10118, the following terms and definitions apply.

**3.1**
**big-endian**
a method of storage of multi-byte numbers with the most significant bytes at the lowest memory addresses

**3.2**
**collision-resistant hash-function**
a hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

NOTE – computational feasibility depends on the specific security requirements and environment.

**3.3**
**data string (data)**
a string of bits which is the input to a hash-function