AS ISO/IEC 10118.3 Supplement 1—2006

Information technology—Security techniques—Hash-functions—Part 3: Dedicated hash-functions—Supplement 1: Dedicated Hash-Function 8 (SHA-224)

(Supplement to AS ISO/IEC 10118.3—2006)

STANDARDS Australia

This Australian Standard Supplement was prepared by Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 8 August 2006.
This Supplement was published on 27 November 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 06303.

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Standards may also be withdrawn.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.

AS ISO/IEC 10118.3 Supplement 1—2006

Information technology—Security techniques—Hash-functions—Part 3: Dedicated hash-functions—Supplement 1: Dedicated Hash-function 8 (SHA-224)

(Supplement to AS ISO/IEC 10118.3—2006)

First published as AS ISO/IEC 10118.3 Supp 1—2006.

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

ISBN 0 7337 7873 9

PREFACE

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

The objective of this Supplement is primary inclusion of Dedicated Hash-Function 8 (SHA-224) to provide the complete family of SHA hash-functions in AS ISO/IEC 10118.3—2006. The description of SHA-224 is given in Clause 14. Test vectors for SHA-224 are given in A.8.

It was noted that there were implementations of SHA-384 and SHA-512 in the field which correctly reproduced the test vector examples in AS ISO/IEC 10118.3 yet still failed for inputs, containing bytes that were not standard ASCII codes. In order to perform comprehensive testing of the SHA-224, SHA-225, SHA-384 and SHA-512 hash functions, an extended set of test vectors is included for AS ISO/IEC 10118.3 as a part of this supplement. This additional test vector information is given in A.9.

This Supplement is identical with, and has been reproduced from ISO/IEC 10118-4:1998/Amd.1:2000, *Information technology—Security techniques—Hash-functions*—Part 3*: Dedicated hash-functions*—Amendment 1: *Dedicated hash-function 8 (SHA-224)*.

This document was originally published as an Amendment by ISO, but it is reproduced here as a supplement with the new material augmenting rather than replacing any in AS ISO/IEC 10118.3.

As this Supplement 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) A full point substitutes for a comma when referring to a decimal marker.

AUSTRALIAN STANDARD

Information technology—Security techniques—Hash-functions—
Part 3:
Dedicated hash-functions
Supplement 1: Dedicated Hash-Function 8 (SHA-224)

Page 22

Add the following after Figure 6.

14 Dedicated Hash-Function 8 (SHA-224)

In this clause we specify a padding method, an initialising value, and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1:2000. The padding method, initialising value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 8. This dedicated hash-function can be applied to all data strings D containing at most 2^{64}-1 bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 8 is equal to 38 (hexadecimal).

NOTE Dedicated Hash-Function 8 defined in this clause is commonly called SHA-224, [2].

14.1 Parameters, functions and constants

14.1.1 Parameters

For this hash-function $L_1 = 512$, $L_2 = 256$ and $L_H = 224$.

14.1.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of clause 10.

14.1.3 Functions

The functions for this hash-function are the same as those for the hash-function of clause 10.

14.1.4 Constants

The constants for this hash-function are the same as those for the hash-function of clause 10.