INTERNATIONAL STANDARD

ISO/IEC 10118-1

Second edition
2000-06-15

Information technology — Security techniques — Hash-functions —

Part 1: General

Technologies de l'information — Techniques de sécurité — Fonctions de brouillage —

Partie 1: Généralités

Reference number
ISO/IEC 10118-1:2000(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 10118 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 10118-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 10118-1:1994), which has been technically revised to add a general model for hash-functions. Note, however, that implementations which comply with ISO/IEC 10118-1:1994 will be compliant with this edition of ISO/IEC 10118-1.

ISO/IEC 10118 consists of the following parts, under the general title *Information technology — Security techniques — Hash-functions*:

— *Part 1: General*

— *Part 2: Hash-functions using an n-bit block cipher algorithm*

— *Part 3: Dedicated hash-functions*

— *Part 4: Hash-functions using modular arithmetic*

Annex A forms a normative part of this part of ISO/IEC 10118.

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