

DRAFT AMENDMENT

ISO/IEC 10118-1:2016/DAM 1

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on:
2020-08-10

Voting terminates on:
2020-11-02

Information technology — Security techniques — Hash-functions —

Part 1: General

AMENDMENT 1: Padding methods for sponge functions

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

Partie 1: Généralités

AMENDEMENT 1

ICS: 35.030

PREVIEW
iTeh STANDARD
(standards.itih.ai)
Full standard:
<https://standards.itih.ai/catalog/standards/sist/be4b222c-4dda-4a04-98cc-cc337756626/iso-iec-10118-1-2016-damd-1>

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/IEC 10118-1:2016/DAM 1:2020(E)

© ISO/IEC 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/be4b4d2c-4dda-4a04-98cc-cc337756626/iso-iec-10118-1-2016-damd-1>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This amendment applies to the third edition (ISO/IEC 10118-1:2016), which has been technically revised.

A list of all parts in the ISO/IEC 10118 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/be4b4d2c-4dda-4a04-98cc-cc337756626/iso-iec-10118-1-2016-damd-1>

Information technology — Security techniques — Hash-functions —

Part 1: General

AMENDMENT 1: Padding methods for sponge functions

AA: Page 6, Annex A

Change this annex to be informative.

BB: Page 6, Clause A.1

Replace last sentence of Paragraph 1 with the following:

Three methods are presented in this annex.

CC: Page 6, After Clause A.3

Add the following Clause A.4:

A.4 Method 3 -- Pad10*1

The data D for which the hash code is to be calculated is padded using the following procedure:

- a) D is concatenated with a single '1' bit.
- b) The result of the previous step is concatenated with $(-m - 2)$ modulo L_1 '0' bits, where m is the original length of D .
- c) Append the single bit '1', yielding the padded version of D .