INTERNATIONAL STANDARD

ISO/IEC 10118-1

Third edition
2016-10-15

AMENDMENT 1

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

PROOF/ÉPREUVE

Reference number
ISO/IEC 10118-1:2016/Amd.1:2021(E)

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.

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 document 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 and IEC 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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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.*

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.

Information technology — Security techniques — Hash-functions —

Part 1: General

AMENDMENT 1: Padding methods for sponge functions

Annex A

Change the status to informative.

A.1, first paragraph

Replace the last sentence with the following:

> Three methods are presented in this annex.

A.4

Add new Clause A.4 as follow:

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.

ICS 35.030

Price based on 1 page