INTERNATIONAL STANDARD

ISO/IEC 20008-2

First edition
2013-11-15
AMENDMENT 1

Information technology — Security techniques — Anonymous digital signatures —

Part 2: Mechanisms using a group public key

AMENDMENT 1

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Technologies de l'information — Techniques de sécurité — Signatures numériques anonymes —

Partie 2: Mécanismes utilisant une clé publique de groupe

AMENDEMENT 1

ISO/IEC 20008-2:2013/PRF Amd 1
https://standards.iteh.ai/catalog/standards/sist/084750b3-dbf4-44b9-81bc-ec4ca3f7a1b2/iso-iec-20008-2-2013-prf-amd-1

PROOF/ÉPREUVE

Reference number
ISO/IEC 20008-2:2013/Amd.1:2020(E)

© ISO/IEC 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 20008-2:2013/PRF Amd 1
https://standards.iteh.ai/catalog/standards/sist/084750b3-dbf4-44b9-8f6c-ec4ca3f7c92e/iso-iec-20008-2-2013-prf-amd-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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 20008-2:2013/PRF Amd 1
https://standards.iteh.ai/catalog/standards/sist/0847750b3-dbfd-44b9-8fbc-ec4ca3f7c92e/iso-iec-20008-2-2013-prf-amd-1

A list of all parts in the ISO/IEC 20008 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.

© ISO/IEC 2020 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 20008-2:2013/PRF Amd 1
https://standards.iteh.ai/catalog/standards/sist/084750b3-dbf4-44b9-8f6c-ec4ca3f7c92e/iso-iec-20008-2-2013-prf-amd-1

Information technology — Security techniques — Anonymous digital signatures —

Part 2: Mechanisms using a group public key

AMENDMENT 1

Clause 5

Add the following to the end of Clause 5:

Annex A lists the object identifiers which shall be used to identify the mechanisms specified in this document.

Annex B defines the special hash-functions which shall be used for the mechanisms specified in this document.

Annex C defines the security guidelines for the anonymous signature mechanisms specified in this document.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Annex D provides a comparison of the revocation mechanisms specified in this document.

ISO/IEC 20008-2:2013/PRF Amd 1
https://standards.iteh.ai/catalog/standards/sist/[illegible]-ec4ca3f7c92e/iso-iec-20008-2-2013-prf-amd-1

Annex E provides numerical examples for each digital signature mechanism specified in this document.

Annex F provides a technique for proof of correct generation for Mechanism 5 of this document.

Annex C

Add new clause C.3 as follows:

C.3 Restrictions on use

Mechanism 6 (see 7.3) should only be used in environments where the group membership issuer and group membership opener are the same entity. The anonymity property can be at risk if the issuer is malicious. For further details, see Reference [20].

Bibliography

Add new bibliographic entry as follows:

[20] ISHIDA. A. et al. Proper usage of the group signature scheme in ISO/IEC 20008-2. *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, AsiaCCS 2019*, pp. 515—528, ACM, 2019

© ISO/IEC 2020 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 20008-2:2013/PRF Amd 1
https://standards.iteh.ai/catalog/standards/sist/084750b3-dbf4-44b9-8f6c-ec4ca3f7c92e/iso-iec-20008-2-2013-prf-amd-1

ICS 35.030
Price based on 1 page

© ISO/IEC 2020 – All rights reserved