
**Information security — Non-
repudiation —**

**Part 1:
General**

Sécurité de l'information — Non-répudiation —

Partie 1: Généralités

**iTeh Standards
(<https://standards.iteh.ai>)
Document Preview**

ISO/IEC 13888-1:2020

<https://standards.iteh.ai/catalog/standards/iso/7444002d-9499-4b9a-beb1-f36ab2ab1875/iso-iec-13888-1-2020>



Reference number
ISO/IEC 13888-1:2020(E)

© ISO/IEC 2020

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO/IEC 13888-1:2020](https://standards.itih.ai/catalog/standards/iso/7444002d-9499-4b9a-beb1-f36ab2ab1875/iso-iec-13888-1-2020)

<https://standards.itih.ai/catalog/standards/iso/7444002d-9499-4b9a-beb1-f36ab2ab1875/iso-iec-13888-1-2020>



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

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	8
4.1 Symbols	8
4.2 Abbreviated terms	9
5 Document organization	9
6 Requirements	9
7 Generic non-repudiation services	10
7.1 Non-repudiation services	10
7.2 Entities involved in the provision and verification of evidence	10
8 Trusted third party involvement	11
8.1 General	11
8.2 Evidence generation phase	11
8.3 Evidence transfer, storage and retrieval phase	12
8.4 Evidence verification phase	12
9 Evidence generation and verification mechanisms	13
9.1 General	13
9.2 Secure envelopes	13
9.3 Digital signatures	13
9.4 Evidence verification mechanism	13
10 Non-repudiation tokens	14
10.1 General	14
10.2 Generic non-repudiation token	14
10.3 Time-stamp token	15
10.4 Notarization token	15
11 Specific non-repudiation services	16
11.1 General	16
11.2 Non-repudiation of origin	17
11.3 Non-repudiation of delivery	17
11.4 Non-repudiation of submission	17
11.5 Non-repudiation of transport	17
12 Use of specific non-repudiation tokens in a messaging environment	18
Bibliography	20

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 <http://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 Joint Technical Committee ISO/IEC JTC 1 *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 13888-1:2009), which has been technically revised.

The main changes compared to the previous edition are as follows:

- [Clause 3](#) has been updated;
- terminology issues have been fixed; and
- a new requirement has been introduced when using hash functions.

A list of all parts in the ISO/IEC 13888 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.