TECHNICAL REPORT

ISO/TR 23244

First edition
2020-05

Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations

Reference number
ISO/TR 23244:2020(E)

© ISO 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO 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
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

 © ISO 2020 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **1**
5 Privacy framework for blockchain/DLT systems ... **2**
5.1 Overview ... 2
5.1.1 General ... 2
5.1.2 Actors and roles ... 3
5.1.3 PII principals ... 3
5.1.4 PII controller ... 3
5.1.5 PII processor ... 3
5.2 Interactions ... 3
5.3 Recognizing PII ... 3
5.3.1 General ... 3
5.4 Privacy safeguarding requirements ... 4
5.4.1 General ... 4
5.4.2 Legal and regulatory factors ... 4
5.4.3 Storage of PII on blockchain and DLT systems ... 5
5.4.4 Contractual factors ... 5
5.4.5 Business Factors ... 6
5.5 Privacy policies ... 6
5.6 Privacy controls ... 7
5.6.1 General ... 7
5.6.2 On-chain and off-chain PII data storage and privacy considerations ... 8
5.6.3 Privacy enhancing technologies applicable to blockchain and DLT Systems ... 9
5.7 Privacy and identity management ... 13
6 Privacy impact assessment ... **13**
6.1 General ... 13
6.2 Privacy impact assessment as part of the overall risk management program ... 13
6.3 Privacy threats ... 13
6.4 Privacy vulnerabilities ... 13
6.5 Privacy consequences ... 14
6.6 Privacy risk mitigation strategies ... 14
7 Privacy management in blockchain and DLT ... **14**
7.1 General ... 14
7.2 Personal information management systems ... 14
7.3 Change management ... 14
7.4 Monitoring, review and continuous improvement ... 15
7.5 PII principal awareness ... 15
7.6 Privacy-related complaint handling ... 15
7.7 Decommissioning ... 16
7.8 Regulatory and compliance aspects ... 16
Bibliography ... **17**

© ISO 2020 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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/TC 307, *Blockchain and distributed ledger technologies,* in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information security,* Subcommittee SC 27, *cybersecurity and privacy protection*.

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 2020 – All rights reserved

Introduction

This document provides an overview of the issues and practical concerns related to privacy and personally identifiable information (PII) protection in the context of blockchain and distributed ledger technologies (DLT) and their applications.

Privacy and PII protection issues are widely considered as a major barrier for the adoption of DLT-based solutions. This document identifies and assesses known privacy-related risks and the way to mitigate them, as well as the privacy-enhancing potential of blockchain and distributed ledger technology.

© ISO 2020 – All rights reserved

Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations

1 Scope

This document provides an overview of privacy and personally identifiable information (PII) protection as applied to blockchain and distributed ledger technologies (DLT) systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22739[1)], *Blockchain and distributed ledger technologies — Terminology*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 29100, *Information technology — Security technique — Privacy framework is referred to in the text in order to provide terms and definitions*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739, ISO/IEC 27000 and ISO/IEC 29100 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Abbreviated terms

The following abbreviations are used in this document:

DLT	distributed ledger technology
EU	European Union
ICT	information and communication technology
IoT	internet of things
PET	privacy enhancing technology
PII	personally identifiable information
ZKSNARK	zero-knowledge succinct non-interactive argument of knowledge

1) Under preparation. Stage at the time of publication: ISO/FDIS 22739:2020.

© ISO 2020 – All rights reserved