TECHNICAL REPORT

ISO/TR 23576

First edition
2020-12

Blockchain and distributed ledger technologies — Security management of digital asset custodians

Reference number
ISO/TR 23576:2020(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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative reference **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Basic description of a model of online system for digital asset custodianship **3**
5.1 General 3
5.2 Example of a system for digital asset custodians and its functional components 3
5.3 Examples of transactions 5
5.4 Description of keys used for signature and encryption 6
5.4.1 Type of keys 6
5.4.2 Flow for key generation and key usage 6
5.4.3 Using multiple keys 8
5.4.4 Suspension of keys 8
5.5 Characteristics of digital assets held in DLT / blockchain systems 8
5.5.1 General 8
5.5.2 Importance of signature keys 8
5.5.3 Diversity of implementations 9
5.5.4 Possibility of blockchain forks 9
5.5.5 Risks for unapproved transactions 10
6 Basic objectives of security management for digital asset custodians **11**
7 Approaches to basic security controls **11**
8 Digital asset custodians' risks **12**
8.1 General 12
8.2 Risks related to the system / platform of the digital asset custodian 12
8.2.1 General 12
8.2.2 Signature key risks 13
8.2.3 Risks on asset data 16
8.2.4 Risks related to suspension of systems and operations 17
8.3 Risks from external factors 17
8.3.1 General 17
8.3.2 Risks related to the internet infrastructure and authentication infrastructure 18
8.3.3 Risks inherent to digital asset DLT systems / blockchains 18
8.3.4 Risks arising from external reputation databases and anti-money-laundering regulations 19
9 Consideration on security controls of digital asset custodians **20**
9.1 General 20
9.2 Basis for considerations about security management 20
9.3 Considerations about security controls on digital asset custodians 21
9.3.1 Guidelines for the information security management 21
9.3.2 Information security policies 21
9.3.3 Organization of information security 21
9.3.4 Human resource security 22
9.3.5 Asset management 22
9.3.6 Access control 22
9.3.7 Security controls on signature keys 24
9.3.8 Physical and environmental security 28
9.3.9 Operations security 28
9.3.10 Communications security 30
9.3.11 Supplier relationships 32

© ISO 2020 – All rights reserved

9.3.12 Information security incident management 32
9.3.13 Information security aspect of business continuity management 32
9.3.14 Compliance 33
9.4 Other digital asset custodian system specific issues — Advance notice to user for maintenance 34
Bibliography **35**

© 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*.

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

A digital asset custodian holds customers' digital assets for safekeeping in order to minimize the risk of their theft or loss. This document illustrates the security risks, threats, and measures which digital asset custodians consider, design, and implement in order to protect the assets of their customers, based on best practices, existing standards and research. For example, the management of signature keys for digital assets requires special attention, taking into account the specific nature of blockchains and DLT systems and the security challenges they face. A key topic discussed is the appropriate management of signature keys by digital asset custodians in order to prevent misuse and transactions by unauthorized individuals.

© ISO 2020 – All rights reserved

Blockchain and distributed ledger technologies — Security management of digital asset custodians

1 Scope

This document discusses the threats, risks, and controls related to:

— systems that provide digital asset custodian services and/or exchange services to their customers (consumers and businesses) and management of security when an incident occurs;

— asset information (including the signature key of the digital asset) that a custodian of digital assets manages.

This document is addressed to digital asset custodians that manage signature keys associated with digital asset accounts. In such a case, certain specific recommendations apply.

The following is out of scope of this document:

— core security controls of blockchain and DLT systems;

— business risks of digital asset custodians;

— segregation of customer's assets;

— governance and management issues.

2 Normative reference

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, *Blockchain and distributed ledger technologies — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739 and the following 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/

3.1
digital asset custodian system
system that holds customers' digital assets for safekeeping in order to minimize the risk of their theft or loss

Note 1 to entry: In this document, holding assets is considered in a broad sense, as it includes for instance, the case of physically or digitally storing the assets, but also the case of holding the private keys associated with the assets, or even the case of protecting access to the assets, like holding one of the keys protecting the access to the assets.

© ISO 2020 – All rights reserved

3.2
cold wallet
cold storage
offline application or mechanism used to generate, manage, store, or use private and public keys

3.3
hot wallet
hot storage
online application or mechanism used to generate, manage, store, or use private and public keys

3.4
hardware wallet
wallet which leverages a hardware device (e.g. HSM) to generate, manage, store, or use private and public keys

3.5
deterministic wallet
wallet in which multiple key pairs are derived from a single starting point known as a seed

3.6
hierarchical deterministic wallet
deterministic wallet (3.5) in which child key pairs are derived from the master key pair

Note 1 to entry: Descendant key pairs can be derived from the child key pairs, in a hierarchical manner, hence the name of the wallet. Child key pairs can be used and shared without having to share the master key pair. It is defined within Reference [7].

4 Abbreviated terms

AML	anti-money laundering
API	application programming interface
APT	advanced persistent threat
CFT	countering financing of terrorism
DLT	distributed ledger technology
DNS	domain name system
FATF	Financial Action Task Force
FQDN	fully qualified domain name
HSM	hardware security module
SMS	short message service
ISMS	information security management system
ISP	internet service provide
KYC	know your customer
OS	operating system
OWASP	Open Web Application Security Project
PII	personally identifiable information

© ISO 2020 – All rights reserved