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 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

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.

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.

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.