TECHNICAL REPORT

ISO/TR 24374

First edition
2023-04

Financial services — Security information for PKI in blockchain and DLT implementations

Reference number
ISO/TR 24374:2023(E)

© ISO 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

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

© ISO 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **2**
5 Relevant issues - Distributed Ledger Technology (DLT) / Blockchain and PKI ... **3**
5.1 DLT/Blockchain data security and privacy concerns ... 3
5.1.1 General ... 3
5.1.2 From centralised to decentralized ... 3
5.1.3 Instant exploitation ... 3
5.1.4 Protecting the key is critical ... 3
5.2 Problems and attacks associated with PKI systems ... 4
5.2.1 Current Challenges of Public Key Infrastructure ... 4
5.2.2 Attacks to PKI ... 4
5.3 Security objectives ... 5
5.4 Summary of the use of asymmetric key cryptography in blockchain networks ... 5
5.5 Private key storage ... 6
6 Security and privacy activities ... **6**
6.1 Cryptographic tools ... 6
6.2 Governance activities ... 7
6.3 Operation activities ... 7
7 Blockchain and DLT controls ... **7**
7.1 Technical Controls ... 7
8 Security and privacy processes ... **8**
8.1 General ... 8
8.2 Standard advice on organisation security and privacy processes ... 8
8.2.1 General ... 8
8.2.2 Standard advice on risk analysis ... 8
8.3 Technical Design Elements ... 9
8.4 Legal Risk ... 9
9 Blockchain based PKI implementations ... **10**
Annex A (Informative) ... **11**
Annex B (Informative) ... **15**
Bibliography ... **17**

© ISO 2023 – 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 68, *Financial Services*, Subcommittee SC 2, *Financial Services, security*.

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 2023 – All rights reserved

Introduction

Even though DLT/Blockchain-based solutions are at a relatively early stage of adoption and significant challenges remain, they hold the potential [7] for major opportunities across several sectors. While the financial sector has shown widespread early interest in DLT/Blockchain, other public and private sector organisations that rely on the keeping of records and management of secure transactions also benefit. DLT/Blockchain also provide opportunities in the healthcare, pharmaceutical, creative, and food sectors.

In light of the growing interest in DLT/Blockchain, standardisation efforts have gathered momentum, particularly with the setting up of the ISO technical committee https://www.iso.org/committee/6266604.html on Blockchain and electronic distributed ledger technologies (ISO/TC 307 Blockchain and distributed ledger technologies).

ISO/DTR 23245 states that: '(i) The essential part of key lifecycle management for blockchain is similar to an ordinary PKI type system (ii) Some blockchain applications do not have the revocation process for the key pair. In such cases different type of key management process is needed.'

Consideration of the major implications and the impact that DLT/ Blockchain will have on current PKI implementations for financial services is essential to minimise any potential disruption.

© ISO 2023 – All rights reserved

Financial services — Security information for PKI in blockchain and DLT implementations

1 Scope

This document describes the management of cryptographic keys in a blockchain, or distributed system used in the financial sector

The objective of this document is to consider the impact of different types of key management processes that are required for PKI implementations in Blockchain and DLT projects

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
blockchain
distributed ledger (3.4) with confirmed blocks organized in an append-only, sequential chain using cryptographic links

Note 1 to entry: blockchains are designed to be tamper-proof and to create final, definitive, and immutable *ledger records* (3.10).

3.2
consensus
agreement among DLT nodes that a) a transaction is validated and b) that the *distributed ledger* (3.4) contains a consistent set and ordering of validated transactions

3.3
consensus mechanism
rules and procedures by which *consensus* (3.2) is reached

3.4
distributed ledger
ledger (3.9) that is shared across a set of DLT nodes and synchronized between the DLT nodes using a *consensus mechanism* (3.3)

[SOURCE: ISO 22739:2020, 3.44]

3.5
distributed ledger technology system
DLT system

system that implements a *distributed ledger* (3.4)

© ISO 2023 – All rights reserved

3.6
distributed ledger technology
DLT
technology that enables the operation and use of *distributed ledgers* (3.4)

3.7
distributed ledger technology node
DLT node
distributed ledger technology device or process that participates in a network and stores a complete or partial replica of the *ledger records* (3.10)

3.8
hardware security module
HSM
hardware implementation of a secure crypto-processor using an ITU-T X.509 certificate and a private key to provide secure authentication (ISO/IEC 19790:2012 security level 3 or higher)

3.9
ledger
information store that keeps records of transactions that are intended to be final, definitive, and immutable

3.10
ledger record
distributed ledger technology record comprising hashes of transaction records or references to transaction records recorded on a *blockchain* (3.1) or distributed ledger system

[SOURCE: ISO 22739:2020, 3.30]

4 Symbols and abbreviated terms

API	Application Program Interface
BCP	Business Continuity Plan
BTC	Bitcoin
CA	Certificate authority
DHT	Distributed hash table
CRL	Certificate Revocation List
DTR	Draft technical report
ETL	Extract, transfer, and load
HSM	Hardware security module
KYC	Know your customer
LDAP	Lightweight Directory Access Protocol
MITM	Man-In-The-Middle
OCSP	Online certificate status protocol
PAX	Paxos Standard
PKI	Public key infrastructure

© ISO 2023 – All rights reserved