ISO/TR 24374
ISO TC 68/SC 2/WG 8
Date: 2022-09-12-02
Secretariat: BSI

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

~~TR stage~~

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

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.orgwww.iso.org

Published in Switzerland

Contents

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. ~~Note~~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 ~~is~~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, ~~SC2, WG8~~*Financial Services,* Subcommittee SC 2, *Financial Services, security*.

~~Direct any~~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

Even though DLT/Blockchain-based solutions are at a relatively early stage of adoption and significant challenges remain, they hold the potential 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 ~~the~~ 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.

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 ~~2~~ Normative references

~~The following documents are referred to in the text in such a way that some or all 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.~~

There are no normative references in this document.

3 ~~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)

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
HSM 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]

54 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

VPN Virtual Private Network

WoT Web of Trust

5

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

VPN	Virtual Private Network
WoT	Web of Trust

65 Relevant issues - Distributed Ledger Technology (DLT) / Blockchain and PKI

6.15.1 5.1 DLT / /Blockchain data security and privacy concerns

5.1.1 General

Blockchain and DLT systems involve nodes on a peer-to-peer network that store data, where the data finality is agreed upon via a consensus mechanism. Each node has a cryptographic module to conduct cryptographic operations as specified in the underlying protocol. Though blockchain networks and services do not have a centralized server, it does not mean protection of a node is not needed. Best efforts to protect each node is an essential part in securing the entire blockchain based system.

At its most basic, blockchain technology projects are a peer to peer based distributed ledger or databased organized by a set of protocols combined with a blockchain, i.e., a series of encrypted sets of data that record immutable changes over time.

One of blockchains greatest assets is its write-once, append many distributed nature; it can be easily deployed across disparate nodes on the web, yet each record contains its own hash making it immutable. To this end, cryptography is the primary meanmeans to protect the applications, networks, infrastructure, and services from cyber-threats. However, the existing Public Key Infrastructurepublic key infrastructure (PKI) is based on a central Certificate Authoritycertificate authority (CA) that can become a bottleneck which will affect the efficiency of the cryptographic protocols because of the overhead incurred by the verification of cryptographic signatures and certificates. Recently, blockchain has also been leveraged to aid PKI without the need for a central authority. But it also creates unique security [7] challenges which are described in clause 5.

6.1.15.1.2 5.1.1 From centralised to decentralized

Blockchain shifts data storage and protection from a centralized to a decentralized model. In traditional centralized models, security methods can be consolidated with the technology products they serve. Blockchain, however, requires innovative security measures to protect the dynamic and highly distributed financial products the technology aims to support.

As with any crypto-based infrastructure, protecting keys is paramount to ensuring a blockchain system's security.

A successful blockchain system needs highly reliable methods of interfacing with the strong key protection practices afforded by HSMs, secure elements, and other computing environments designed for secure execution of code, and all of these deliver the scaling and flexibility a decentralized blockchain model needs.

6.1.25.1.3 5.1.2 Instant exploitation

Anyone who obtains the key can monetize and exploit the asset instantly. As seen in security breaches in public blockchain settings, such as Bitfinex, Mt. Gox and others, the malicious transfer of 'value' can be instantaneous, irreversible, and significant. Participants in these systems lost millions of dollars because of compromised security systems. However, note that these attacks exploited vulnerabilities at the application layer—the wallets holding the keys to the assets—rather than the underlying blockchain

