TECHNICAL REPORT

ISO/TR 24374

First edition

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7c3a8b3/iso-prf-tr-24374

PROOF/ÉPREUVE

Reference number
ISO/TR 24374:2023(E)

© ISO 2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7c3a8b3/iso-prf-tr-24374

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

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d665d7e3a8b3/iso-prf-tr-24374

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 24374

© 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 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7c3a8b3/iso-prf-tr-24374

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7c3a8b3/iso-prf-tr-24374

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/

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7e3a8b3/iso-prf-tr-24374

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]

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7c3a8b3/iso-prf-tr-24374

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

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 means to protect the applications, networks, infrastructure, and services from cyber-threats. However, the existing public key infrastructure (PKI) is based on a central certificate 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7c3a8b3/iso-prf-tr-24374

5.1.2 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.

5.1.3 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 protocol. So far, blockchain technology itself has proved tamper-proof, within the limits presented by the consensus mechanism adopted by the network.

5.1.4 Protecting the key is critical

The ability to add transactions to a transaction database broadens the technology's applicability.

Traditional PKI is CA based, so the security of PKI systems are at risk if one CA is compromised For example, a framework mitigates the problems with PKI such as the difficulties with rapid certificate revocation, elimination of single points of failure and CAs' malfunctions. Note that If the root CA were to be compromised, an attacker could gain control of the entire PKI and compromise trust in the entire system, including any sub-systems reliant on the PKI.

5.2 Problems and attacks associated with PKI systems

5.2.1 Current Challenges of Public Key Infrastructure

The most commonly employed approach to PKIs is the Web PKI. It is a Certificate Authority based system that adopts a centralized trust infrastructure. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. Verification is required to check the authenticity of the party with whom the secure connection is established. The most important task is to establish the correspondence between the identity (identification data) and the user's public key. This problem is solved using a public key certificate — an electronic document used to prove ownership of a public key. The certificate contains the public key and user credentials, as well as the electronic signature of the trusted party that verifies the user. To ensure the integrity and authenticity of the certificate, it is signed by a trusted party – a certification authority.

Centralized Web PKI solutions have several significant problems.

a) There are some challenges associated with quick notification of key compromise, since the formation and distribution of the list of revoked certificates can take from several minutes to an hour, unless synchronous verification protocols like OCSP are used. As a result, there is no 100% guarantee that this key is still valid. This problem is also relevant for DLT systems, where a transaction could be signed by a key that is no longer valid or under the sole responsibility of the owner. If the certificate is verified online (by request to the certification authority), then the user's privacy is violated, since the certification authority will know the entire history of user interaction.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7c3a8b3/iso-prf-tr-24374

b) The definition of the list of trusted CAs in a PKI system could be complex and could require some specific out-of-protocol management, although successful collaborations have resulted in highly-federated environments, like the European Trusted Services List. A decentralized system could also be impacted by this problem.

c) The centre of the system is always an attack point and compromising the root certificate will expose the entire system to a bunch of vulnerabilities.

d) Identifier management is in the hands of a centralized organization and does not belong to the identifier owner himself.

There are significant sources of failures of PKI that neither the usability nor traditional computer security community is engaging. Specifically, there are incidents that illustrate systematic weaknesses of organizational practices that create risks for all who rely upon PKI. However, there are organizational and configuration choices that could avoid or mitigate some of these risks.[15]

In decentralized PKI, blockchain can act as a decentralized key-value storage. It is capable of securing the data read to prevent MITM (Man-In-The-Middle) attacks, and to minimize the power of third parties.

5.2.2 Attacks to PKI

PKI is exposed to risks due to potential failures of certificate authorities (CAs) that can be used to issue unauthorized certificates for end-users. Many breaches show that if a CA is compromised, the security of the corresponding end-users will be in risk. There are many cases where a CA's errors or breaches have resulted in unauthorized certificates being issued.[12]

Another important weakness of PKIs concerns the reliability and security of certificate revocation lists (CRLs or associated OCSP servers), which are used to ensure proper lifecycle management of

© ISO 2023 – All rights reserved

certificates, particularly the revocation, and are to be queried any time a certificate is used. Classically, the CRL for a set of certificates is maintained by the same (and sole) certification authority (CA) that issued the certificates, and this introduces a single point of failure into the system.

In fact, CRLs do not operate in real time; they are commonly updated periodically by the issuing CA, and there can be a delay between a security breach and the subsequent CRL update, resulting in the temporary use of compromised certificates. The theft of a certificate (with its associated private key) could be unknown to the CA, and the certificate is not revoked in this case.[10] See Annex A for possible solutions.

5.3 Security objectives

DLTs that use cryptographic PKI as their security mechanism are resistant to attackers who are not in possession of the appropriate keys. This, in addition to the shared data and tamper-resistant properties of blockchain solutions, means that DLTs have a high level of security. For this reason, provided that controls, see Annex B, such as key management follow industry best practice, DLTs are potentially [7] more robust from a cybersecurity perspective than systems relying on physical or network security, or which are locked with manually-generated passwords rather than cryptographic private keys. DLT also presents integration challenges with hardware security modules (HSMs) for key storage and generation, and security infrastructure such as virtual private networks (VPNs).

HSMs provide limited mechanisms for detection of key misuse, e.g., data encryption versus PIN encryption, signature keys versus encryption keys. DLTs could be based on cryptographic schemes that are not necessarily supported by HSMs, secure elements, nor properly managed by other security components, and that need to consume and process information signed with those keys Also if an attacker compromises a system or application that has permissions to use keys in the HSM, or if a rogue insider abuses such permissions, this will give them the ability to sign fraudulent cryptocurrency transactions. One such signature is enough to empty all cryptocurrency in a specific address[10].

Integration challenges with DLTs relate to their security model, which is largely based on PKI (public key infrastructure)[10]. Access rights to writing blockchain state data typically require data transactions to be signed by a specific private key, while reading blockchain state data requires access to either the ledger file (stored on several servers) or access to the interface mechanisms placed over the blockchain data. These interfaces are typically secured via a network credential system (linked to the corporate directory) or a custom password authentication mechanism. Note this varies between DLT systems and in fact does not exist for public permissionless DLT systems.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 24374
https://standards.iteh.ai/catalog/standards/sist/7070d618-6133-4f89-8ca7-d6b5d7c3a8b3/iso-prf-tr-24374

Security mechanisms are an important consideration when integrating highly secure, cryptographically-based blockchain security protocols with other, potentially looser access and control rules in existing legacy systems. Integration from a data point of view is relatively straightforward via standard programming interfaces, assuming that the data integration takes place within the established security framework and standard ETL processes. Once blockchain systems have a secure standard interface, (to be defined) they essentially become another enterprise component, albeit with the unique properties of DLT systems - specifically the immutable record of transactions in a decentralised network where peer nodes share data, assets, and value.

Blockchains can also be used to secure the data in other systems. For example, database backups can be timestamped with a hash of the data to ensure integrity of the backups for regulatory purposes.

Cryptographic approaches such as Merkle trees, make it possible to secure large amounts of data at an individual data row level, A Merkle tree separates the validation of the data from the data itself — the **Merkle** tree can reside locally, or on a trusted authority, or can itself reside on a distributed system.

5.4 Summary of the use of asymmetric key cryptography in blockchain networks

Here is a summary of the use of asymmetric-key cryptography in many blockchain networks.

- Private keys are used to digitally sign transactions.
- Public keys are used to derive addresses.