TECHNICAL REPORT

ISO/TR 23644

First edition
2023-05

Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management

Reference number
ISO/TR 23644:2023(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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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*, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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

In recent years, new decentralized digital identity management systems have emerged, some of them based in distributed ledger technologies (DLTs) providing support functions. As explained in ISO/TR 23249, these include associating identifiers with public keys, supporting the attestation of credentials, enabling credentials revocation, defining common credential templates or implementing trust anchors.

DLT systems provide and rely on different types of trust anchors for DLT-based identity management, each being important in terms of some dimension of policy, technology, data, security, assurance, etc. Each trust anchor presents opportunities and risks to a DLT-based identity management system, and the DLT-based identity management system actors need guidance and standards to develop an appropriate operating model and risk mitigation strategy.

However, the DLT-based identity management system actors have also to take into account risks, including those shared with other organizations in chains of trust, and to have a governance model that is suitable for distributed and decentralized ecosystems formed by multiple actors. The DLT-based identity management system actors have to consider technological change and new types of technology with new risks that can address, create or result in opportunities and threats. The overall effectiveness of the DLT-based identity management system is critically dependent on the quality of the data it holds and shares; this is a high priority in DLT-based identity management system governance and operational models.

This document provides an overview of trust anchors for DLT-based identity management systems.

Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management

1 Scope

This document describes concepts and considerations on the use of trust anchors for systems leveraging blockchain and distributed ledger technologies (DLTs) for identity management, i.e. the mechanism by which one or more entities can create, be given, modify, use and revoke a set of identity attributes.

2 Normative references

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 22739:2020, *Blockchain and distributed ledger technologies — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739:2020 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/

4 Abbreviated terms

AML	anti-money laundering
BIP	bitcoin improvement proposal
CA	certification authority
CAB	Certification Authority Browser (CA/Browser)
DID	decentralized identifier
DKMI	decentralized key management infrastructure
DKMS	decentralized key management system
DLT	distributed ledger technology
eIDAS	electronic identification, authentication and trust services
ETSI	European Telecommunication Standards Institute
EU	European Union
ID	identity

IDP	identity provider
IETF	Internet Engineering Task Force
IoT	internet of things
IP	internet protocol
KERI	key event receipt infrastructure
KYC	know your customer
LoA	level of assurance
LoIP	level of identity proofing
MPC	multi-party computation
OID	object identifier
PDP	policy decision point
PKI	public key infrastructure
RFC	request for comments
RP	relying party
SED	self-encrypting drive
SSI	self-sovereign identity
ToIP	trust over IP
TPM	trusted platform module
UID	unique identifier
VC	verifiable credential
ZKP	zero knowledge proof
ZVE	zero knowledge proof verification engine

5 Types of trust anchors

5.1 Overview

Identity management is defined in ISO/IEC 24760-1:2019, 3.4.1, as the “processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain”. ISO/IEC 24760-1:2019, 3.1.2, defines identity as a “set of attributes related to an entity”, and ISO/IEC 24760-1:2019, 3.1.3, defines an attribute as a “characteristic or property of an entity”. Parties involved in identity management, such as relying parties (RPs), typically have trust relationships among them based in various features, which can be collectively designated as trust anchors.

There is no single definition of a trust anchor because it can mean different things to different people.

NOTE Some authors identify different types of trust anchors, including government trust anchors (i.e. see Reference [38]).

However, for the purposes of this document, the following five different types of trust anchor are described that exist within any governance model, even if they are not obvious (there can be more):

— Legal trust anchors are the trust anchors established and/or recognized by the legislation and regulations of relevant jurisdictions, by the contractual agreements and organizational by-laws. They set a legal foundation for the trust frameworks and underpin the operating rules and procedures. Legal trust anchors can mention or include references to other trust anchors.

— Data trust anchors are authoritative data sources that relate to the entities and attributes to be processed, where very high data quality is vitally important.

— Cryptographic trust anchors, which provide the roots of cryptographic trust and enable cryptographic binding, revocation, authentication, signing, encryption and other trust functions.

— Cybersecurity trust anchors, which monitor, detect and respond to policy violations, and enforce policy compliance. This includes assurance, testing and certification regimes, possibly augmented by the combined effort of a group responsible for defending an enterprise's use of information systems by maintaining its security (so-called "blue team"), known to the defenders, and a group of mock attackers ("red team"), unknown to the defenders.

— Social trust anchors. Subjective trust anchors can exist, particularly in the context of social situations and informal relationships where each individual can have a different view on the assessed risks and the requirements for risk mitigation or legal remedy.

In this document, reference is made to different levels of assurance, borrowed from ISO/IEC 29115 and reflected in other ISO and ISO/IEC standards (maybe using different words) in order to provide a spectrum of risk mitigation measures in response to internal, external and shared risks. Broadly speaking, these are as follows:

a) Level 1. Low assurance. Little confidence in identity, cybersecurity, counter fraud, data quality, etc. No significant risk mitigation strategy. No government-issued identity (ID) documents. Requires repeatability, e.g. user ID, email address. Major use case: social media.

b) Level 2. Medium assurance. Medium confidence. Consumer-centric low-cost risk mitigation strategy for low-value financial risks. Expect failures. Some/increasing use of government-issued ID documents. Major use case: consumer credit/debit cards.

c) Level 3. High assurance. High confidence. Strong risk mitigation strategy to address financial and non-financial risks, with the goal of preventing failures. Good use of government-issued ID documents and real-time authentication/validation. Major use case: employer/employee binding for employees acting digitally internally and externally on behalf of the organization.

d) Level 4. Very high assurance. Very high confidence. Multiple government ID documents or real-time authentication/validation. Major use cases involve danger to life, public safety, high economic risk and national security.

There are other ways to convey this information, such as vectors of trust, as defined in IETF RFC 8485, that essentially provide the assurance information in a more granular way, considering different components or categories of information relevant in the context of authentication processes.

5.2 Legal trust anchors

Trust frameworks exist to describe the policies, procedures and mechanisms for the operation of digital trust across a community of trust, whether that exists in a legally binding agreement or whether it is mandatory across the nation or jurisdiction under the rule of law. In almost all cases, the starting point for a trust framework is the legal baseline upon which a policy framework is built, which forms the core of the trust framework. These policies, based upon legislation, are encapsulated and implemented in rulesets within the technological system, which are controlled through architectural components such as policy decision points (PDPs) and policy enforcement points (PEPs). Legal trust anchors underpin the operating rules.

Examples of relevant legislation include:

— national policy and infrastructure;

— national security;

— financial regulation, anti-money laundering (AML), counter fraud, Revised Payment Service Directive (PSD2, Directive (EU) 2015/2366), Markets in Financial Instruments Directive 2 (MiFID 2, Directive (EU) 2014/65);

— property regulation, real estate, intellectual property;

— privacy and other human rights; General Data Protection Regulation (GDPR, Directive (EU) 2016/679), Network Information Security (NIS) Directive 2 (Directive (EU) 2022/2555);

— identity, US Real ID Act, electronic identification, authentication and trust services (eIDAS, EU Regulation 910/2014).

NOTE Legislation and government policy can refer to international and national standards for guidance and normative controls.

Many forms of integration of a legal trust anchor into DLT based identity systems are possible. For example, a smart contract that queries legal trust anchors for sanctioned accounts can be used as an input to PDPs.

5.3 Data trust anchors

Several major technologies are emerging to provide new opportunities and new risks; all are driven by and depend critically on high quality data. They can't function properly, or at all, without assured high quality data. One or more measures or levels of data quality can be used to indicate relevant properties, such as timeliness, completeness, uniqueness, accuracy and authority. Any or all of these can be combined in a matrix to give a vector or vectors for data quality assurance.

Any trusted system requires access to high quality data from authoritative data sources. These authoritative data sources can be trust anchors, upon which the overall trust framework and the operational system depend. The term "authoritative" usually means that the data are legally admissible in a court of law, and there is a presumption of its reliability. For example, ISO/IEC TS 29003:2018, 3.3, defines authoritative party as an "entity that has the recognized right to create or record, and has responsibility to directly manage, an identifying attribute".

There is a second kind of data trust anchor, which is the register for a unique identifier (UID) and attributes bound to that identifier. This UID register is normally be considered an authoritative source under either legislation or contract law.

EXAMPLE 1 Each nation has a national passport office that is appointed in law to issue passports with a passport number. The passport office is the authoritative source for passport numbers and associated attributes, although an attribute such as date of birth can come from a date of births and deaths register, which is also a legally appointed authoritative source.

EXAMPLE 2 A community of interest such as a supply chain can have a community contract that specifies Company X as the authoritative source for a UID, which is used throughout the supply chain.

The relationship between the two organizations in Example 1 is a chain of trust. Chains of trust normally work forward and are validated backwards. The passport can be issued if the person is recorded as born but not dead in the births and deaths register. Once the person is recorded as dead, then the register immediately notifies the revocation of the "living" attribute to the passport authority, which revokes the passport. Extending the chain, a living person relies upon their passport to prove their identity to their employer who issues an employee ID – Identifier to the person. If the person's passport is reported stolen, their employee ID – Identifier can be revoked.

Important data trust anchors include the following, each of which can support many business use case scenarios and functional use cases:

— organization registers for companies, partnerships, non-profits, charities, government organizations, police, etc.;

— high assurance government registers for citizen ID and resident ID: passports, eID cards, benefits payments, pension payments, tax payments, voting registers, military ID, police ID, driving licences, firearm licences, etc.;

— other government registers for persons, including foreign workers, asylum seekers and refugees;

— health patient records and prescription drug purchases;

— land, building, postal and mapping registers for proof of location;

— databases of utility companies for proof of address;

— financial know your customer (KYC) and AML registers for bank accounts and other related assets;

— domain name registers for domain names and, through the CAB Forum, secure sockets layer (SSL);

— internet service providers for internet protocol (IP) address and locator/identifier separation protocol (LISP) mappings;

— telecommunication companies for phone [international mobile equipment identity (IMEI)] and subscriber identity module (SIM) [international mobile subscriber identity (IMSI)];

— certificate authorities for public key infrastructure (PKI) certificates and policy object identifier (OID) arc references.

5.4 Cryptographic trust anchors

Cryptographic trust anchors provide the roots of cryptographic trust, bind entities and attributes to data subjects and data principals, as well as to actors (direct persons and delegates, either automated or otherwise) within the systems that operate the trust framework.

The certificate issuance and management life cycle, as well as the governance model, are important for most types of centralized and distributed identity management systems. There are identity management systems that do not use public key certificates.

Different examples of cryptographic trust anchors include using a DLT to bind public keys used to control decentralized identifiers (DIDs) to users, or to validate anonymous identity credentials.

5.5 Cybersecurity trust anchors

As with any infrastructure and the people who operate it, there usually exists a risk management model and a cybersecurity framework. The risk management model addresses the main areas of risk management in accordance with ISO 31000, ISO/IEC 27001 and ISO/IEC 27005 or other standards such as NIST SP 800-53, as follows:

— Identify: The identification of risks.

— Prevent: This includes risk assessment and risk treatment, using options such as risk transfer and risk mitigation, and the monitoring of any remaining risks.

— Detect: Prevention is never 100 %. Its purpose is to buy time to detect threats and incidents, and to respond.

— Respond: The response to a detected threat aims to contain and defeat it, ensuring at the same time business continuity.

— Recover: The risk mitigation strategy includes a recovery to normality.

The risk mitigation strategy can include a range of controls, backed by a cybersecurity framework. ISO/IEC TS 27110 provides the guidelines for developing a cybersecurity framework.

Blockchain and DLT raise additional requirements and challenges regarding cybersecurity. These additional requirements cover the following several important areas:

— the cybersecurity policy framework for the distributed or decentralized blockchain/DLT, based upon existing legal requirements;

— the governance model for the maintenance, implementation, operation and enforcement of the cybersecurity policy framework;

— the ecosystem of DLT use cases, conforming to existing jurisdictional and regulatory requirements;

— the consensus model, whether based on lottery or voting (if based on voting, this includes the authentication and authorization model, backed by an audit trail;

— the node architecture, implementation and operation;

— the incident management plan for attacks or incidents affecting the blockchain/DLT.

There are trust anchors that operate as both cryptographic and cybersecurity trust anchors.

EXAMPLE Self-encrypting drives (SEDs) have an internal trusted platform module (TPM), attestation key and cryptographic store separate from the TPM in any other device. The SED can hold the last "known good" state of its host device (e.g. laptop) and provide a secure reference at boot time. If the SED TPM reports an error, then the parent device will not start its operating system. Similarly, if the SED (or another SED) is held on the network, then the basic input/output system (BIOS) layer on the connecting device will validate with the SED on the network for the last known good state of the connecting device. If there is an error, then the laptop will not be allowed to connect to the network; the network policy is that "only known good devices" can connect to the network.

Each community of trust, and the organizations within it, depend on effective collaborative governance of the community and also corporate governance within each organization. Individually and collectively, the following possibilities are considered:

— a governance model of policies and procedures to describe how the community and each organization is going to behave and work;

— a governance organizational structure to develop, operate and enforce the governance model;

— technological and digital mechanisms to make the procedures and processes efficient, effective, re-usable, enforceable and policy compliant;

— establishment of trust anchors for the mechanisms to use.

ISO 37000:2021 gives guidance on the governance of organizations. ISO/IEC 38500 provides guiding principles, and ISO/IEC TR 38502 provides information on a framework and model on the use of information technology (IT) within an organization. ISO/IEC 27014 gives guidance on concepts, objectives and processes for the governance of information security for an organization. A comprehensive governance model considers the above standards including others.

5.6 Social trust anchors

The trust anchors described in 5.2 to 5.5 are all objective in the sense that they are governed by defined legislations, regulations, rules and standards, which have normative requirements reflected in a governance structure that addresses collective risks in a defined manner.

However, other subjective trust anchors can exist, particularly in the context of social situations and informal relationships where each individual can have a different view on the assessed risks and the requirements for risk mitigation or legal remedy. These are described as "social trust anchors".

