ISO ~~TR~~ /DTR 23644:~~2022(X~~2023(E)

Date: 2023-01-19

ISO TC 307/~~JWG4~~JWG 4

Secretariat: ~~XXXX~~SA

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

~~TR 23644~~

~~**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-1214 Vernier, Geneva
Phone: + 41 22 749 01 11
Email: copyright@iso.org
Website: www.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. 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 ~~on~~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~~the following URL:~~.

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 ~~decentralised~~decentralized digital identity management systems have emerged, some of them based in distributed ledger technologies (~~DLT~~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 ~~and more~~, 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 ~~appropriated~~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 ~~organisations~~organizations in chains of trust, and to have a governance model that is suitable for distributed and ~~decentralised~~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 ~~will be~~is a high priority in ~~the~~ 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 ~~provides~~describes concepts and considerations on the use of trust anchors for systems leveraging blockchain and distributed ledger technologies (~~DLT~~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

~~There are no normative references in this document.~~

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 ~~terminological~~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~~anti-money laundering
~~BIOS~~	~~Basic input/output system~~
BIP	~~Bitcoin Improvement Proposal~~bitcoin improvement proposal
CA	~~Certification~~certification authority
CAB	~~Forum~~ Certification Authority Browser (CA/Browser ~~Forum~~)
DID	~~Decentralized~~decentralized identifier
DKMI	decentralized key management infrastructure
DKMS	~~Decentralized~~decentralized key management system
DLT	~~Distributed~~distributed ledger technology
~~DKMI~~	~~Decentralised key management infrastructure~~

~~DPKI~~	~~Decentralised public key infrastructure~~
~~DoD~~	~~United States Department of Defense~~
~~EBSI~~	~~European Blockchain Services Infrastructure~~
eIDAS	~~Electronic~~electronic identification, authentication and trust services
~~EEA~~	~~European Economic Area~~
~~EMV~~	~~Europay Mastercard Visa~~
ETSI	European Telecommunication Standards Institute
EU	European Union
~~FBCA~~	~~Federal Bridge Certification Authority~~
~~GDPR~~	~~EU General Data Protection Regulation~~
~~GF~~	~~Governance framework~~
ID	~~Identity~~identity
IDP	~~Identity~~identity provider
IETF	Internet Engineering Task Force
~~IMEI~~IoT	~~International Mobile Equipment Identity~~internet of things
~~IMSI~~	~~International Mobile Subscriber Identity~~
IP	~~Internet~~internet protocol
KERI	~~Key~~key event receipt infrastructure
~~KERL~~	~~Key event receipt logs~~
KYC	~~Know~~know your customer
~~LACS~~	~~Logical access control system~~
~~LISP~~	~~Locator/identifier separation protocol~~
LoA	~~Level~~level of assurance
LoIP	~~Level~~level of identity proofing
~~MIFID~~	~~EU Markets in Financial Instruments Directive~~
MPC	~~Multi~~multi-party computation
~~MSP~~	~~Membership service provider~~
OID	~~Object~~object identifier
~~PACS~~	~~Physical access control system~~
PDP	~~Policy~~policy decision point
~~PEP~~	~~Policy enforcement point~~
PKI	~~Public~~public key infrastructure

RFC	~~Request~~request for comments
RP	~~Relying~~relying party
SED	~~Self~~self-encrypting ~~drives~~drive
~~SGX~~	~~Security guard extensions~~
~~SIM~~	~~Subscriber identity module~~
SSI	~~Self~~self-sovereign identity
~~SSL~~ToIP	~~Secure sockets layer~~trust over IP
~~TAMP~~	~~Trust anchor management protocol~~
~~TEE~~	~~Trusted execution environment~~
TPM	~~Trusted~~trusted platform module
~~TS~~	~~Technical specification~~
UID	~~Unique~~unique identifier
~~UNCITRAL~~	~~United Nations Commission On International Trade Law~~
~~URL~~	~~Uniform resource locator~~
VC	~~Verifiable~~verifiable credential
~~XSD~~	~~XML schema definition~~
ZKP	~~Zero~~zero knowledge proof
ZVE	~~Zero~~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~~. The same document~~". 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[1]~~.~~.

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 ~~could~~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

[1] ~~Some authors identify different types of trust anchors, including government trust anchors (i.e. see https://medium.com/coinmonks/what-is-a-trust-anchor-in-the-web-of-trust-a763d130f6ba).~~

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 ~~may~~can exist, ~~particular~~particularly in the context of social situations and informal relationships where each individual ~~may~~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~~levels of ~~Assurance~~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.~~ 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.~~ 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.~~ 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 ~~organisation~~organization.

d) Level 4. Very ~~High Assurance.~~ 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~~vectors of ~~Trust~~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~~policy decision points (PDPs) and ~~Policy Enforcement Points~~policy enforcement points (PEPs). Legal trust anchors underpin the operating rules.

Examples of relevant legislation include:

— ~~National~~national policy and infrastructure;

— ~~National~~national security~~.~~;

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

— ~~Property~~property regulation~~. Real~~, real estate, intellectual property~~.~~;

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

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

~~Note that legislation~~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 ~~is~~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 ~~an~~ "authoritative party" as an "entity that has the ~~recognised~~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 ~~would~~is normally be considered an authoritative source under either legislation or contract law. ~~For example, each~~

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~~, may~~ can come from a date of births and deaths register, which is also a legally appointed authoritative source.

~~In a second example, a~~ EXAMPLE 2 A community of interest such as a supply chain~~, could~~ canhave a community contract that specifies Company X as the authoritative source for a ~~unique identifier~~UID, which is used throughout the supply chain.

The relationship between the two ~~organisations~~organizations in ~~the first example~~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 ~~could~~can be revoked.