TECHNICAL REPORT

ISO/TR 23249

First edition
2022-05

Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management

Reference number
ISO/TR 23249:2022(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 ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **1**

5 Existing taxonomies and conceptual architectures ... **3**

5.1 General ... 3

5.2 NIST Taxonomic approach for blockchain IDMS ... 3

5.2.1 General ... 3

5.2.2 Authority model ... 3

5.2.3 Custody and delegation ... 4

5.2.4 Identifier origination schemes ... 5

5.2.5 Credential architectures ... 6

5.3 Functional role of DLT in identity systems ... 7

5.4 Trust Over IP Foundation ... 7

6 Existing DLT systems for identity management ... **7**

6.1 General ... 7

6.2 uPort ... 7

6.3 Decentralized Identity Foundation (DIF) ... 9

6.4 Alastria ID ... 10

6.5 European Self Sovereign Identity Framework (ESSIF) ... 13

6.6 Sovrin^{TM} Network, Hyperledger Indy, Hyperledger Aries and Hyperledger Ursa ... 15

6.7 WEF Known Traveller Digital Identity (KTDI^{TM}) ... 20

6.8 WeIdentity ... 24

6.9 Masterchain ... 25

6.9.1 General ... 25

6.9.2 Actors in the system ... 27

6.10 LACChain ... 27

6.11 Decentralised digital architecture based on blind signatures ... 29

6.11.1 General ... 29

6.11.2 Actors in the system ... 30

6.11.3 Functions in the system ... 30

6.11.4 Flow of messages in the system ... 31

7 Existing relevant standards and frameworks ... **32**

Bibliography ... **37**

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 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

The target audience of this document includes but is not limited to academics, solution architects, customers, users, developers, regulators, auditors and standards development organizations.

Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management

1 Scope

This document provides an overview of existing DLT systems for identity management, i.e. the mechanisms by which one or more entities can create, receive, modify, use and revoke a set of identity attributes.

This document covers the following topics:

— Managing identity for individuals, organizations, things (IoT & objects), functions and processes and other entities including within and across DLT systems.

— Description of the actors and their interactions and common interfaces.

— Architectures.

— Existing relevant standards and frameworks.

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, *Blockchain and distributed ledger technologies — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739 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
BCOS	Be Credible, Open & Secure
BSP	Biometric Service Providers
CCG	Credentials Community Group
CHAPI	Credential Handler API
CMS	Confidential Messaging Service
DID	Decentralized Identifier

DIF	Decentralized Identity Foundation
DKMS	Decentralized Key Management System
DLT	Distributed Ledger Technology
EBSI	European Blockchain Services Infrastructure
eIDAS	EU Regulation on electronic Identification, Authentication and trust Services
ERC	Ethereum Request for Comments
ESSIF	European Self Sovereign Identity Framework
FISCO	Financial Blockchain Shenzhen Consortium
GDPR	EU General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	identity
IDMS	Id Management System
INATBA	International Association for Trusted Blockchain Applications
IPFS	InterPlanetary file system
JSON	JavaScript object notation
JSON-LD	JSON Linked Data
JWT	JSON Web Token
KTDI™	Known Traveller Digital Identity
KYC	Know Your Customer
NIS	Network and Information Systems
PKI	public key infrastructure
SDK	software development kit
SIOP	Self-issued OpenID Provider
SSI	Self-Sovereign Identity
RFC	Request for Comments
ToIP	Trust over IP
TOOP	The Once Only Principle
URI	Uniform Resource Identifier
VC	Verifiable Credentials
W3C	World Wide Web Consortium

WebKMS	Cryptographic Key Management Systems for the Web
ZCAP-LD	Authorization Capabilities for Linked Data
ZKP	Zero Knowledge Proof

5 Existing taxonomies and conceptual architectures

5.1 General

This clause contains existing taxonomies and conceptual architectures, in the form of a list of examples, which is not intended to be exhaustive.

5.2 NIST Taxonomic approach for blockchain IDMS

5.2.1 General

Reference [4] provides an example of a taxonomic approach to understand emerging blockchain identity management systems as a National Institute of Standards and Technology (NIST) publication. It highlights the different features and characteristics that are possible, also exploring the opportunities, challenges and risks associated.

5.2.2 Authority model

There are two main approaches for the authority model, which is the way the system is controlled:

— Top-down: A system owner acts as a central authority that has control over identifier origination and/or credential issuance. This power could be delegated to create a hierarchical structure.

— Bottom-up: There is no single entity acting as a central authority that has control over identifier origination and/or credential issuance. Participants create and manage their own identifiers and credentials without the need of any permission, although they need to follow the (technical) rules of the identity systems.

There are different schemes for identifier origination. An identifier is originated starting from the generation of a blockchain address directly by the user who controls the custody of the associated private keys, usually with the generation of a public/private key pair and then deriving a blockchain address from the public key using a cryptographic hash function and some protocol-specific transformations. There are also additional identifier origination schemes that do not start with the generation of a blockchain address but rather reference the address after generation.

Different methods could be used to originate identifiers, as shown in Figure 1 (reproduced with permission from NIST): schemes that involve no initial registration or self-registration are on the left of the figure. The rightmost box labelled with “By a central authority” represents a top-down authority model. The schemes in-between are other possible alternatives.

In the top-down approach, credentials and/or identifiers are issued by a central authority (a corporate office, a central government), while in the bottom-up they are issued by any user to another user, or directly issued by a user to themselves.

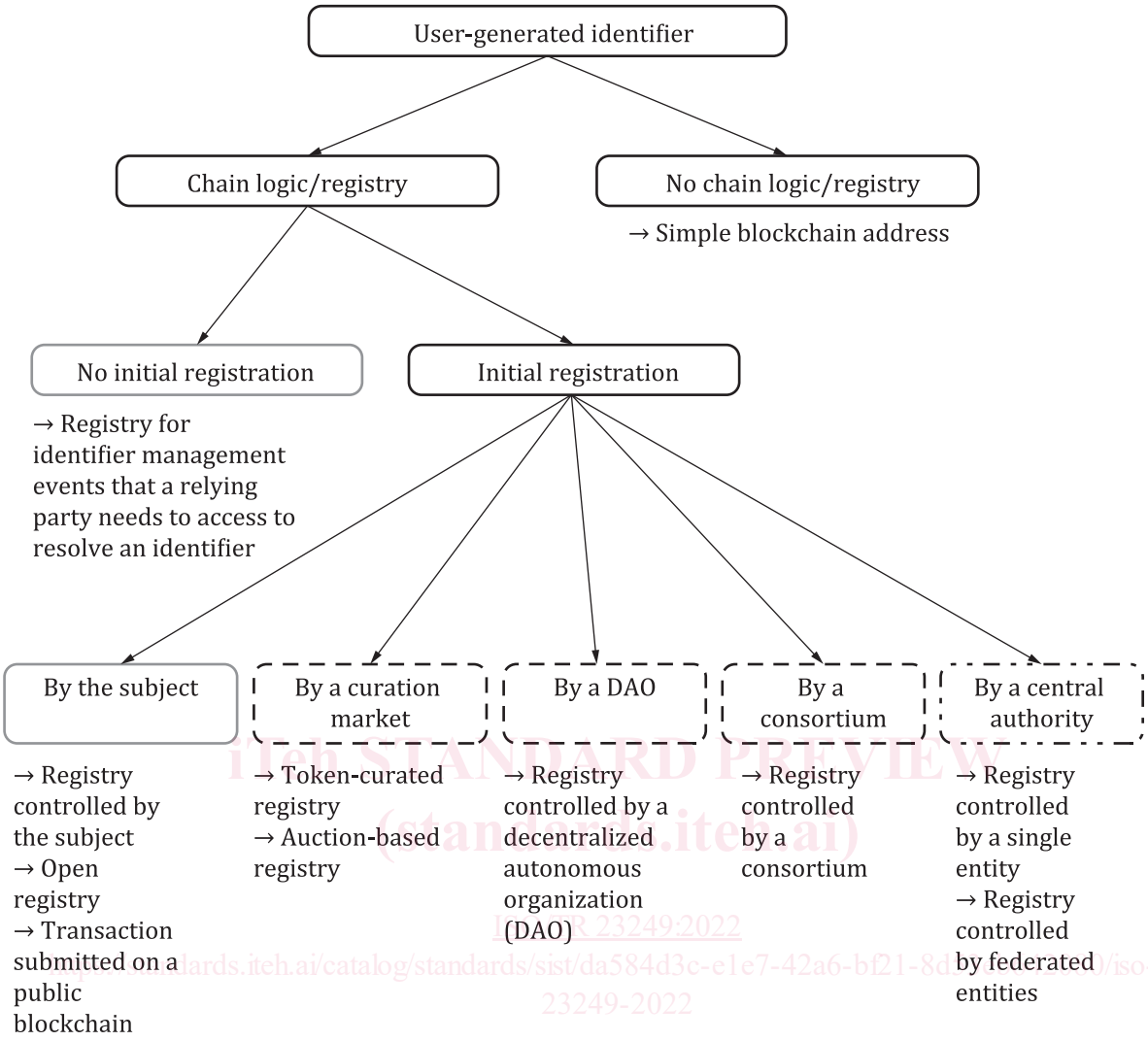

Figure 1 — Identifier origination schemes

5.2.3 Custody and delegation

Figure 2 (reproduced with permission from NIST) shows different interactions between entities and an identity management system; these interactions are either direct or delegated through custodian (in this context, a datastore is an off-chain personal storage linked with a given identity).

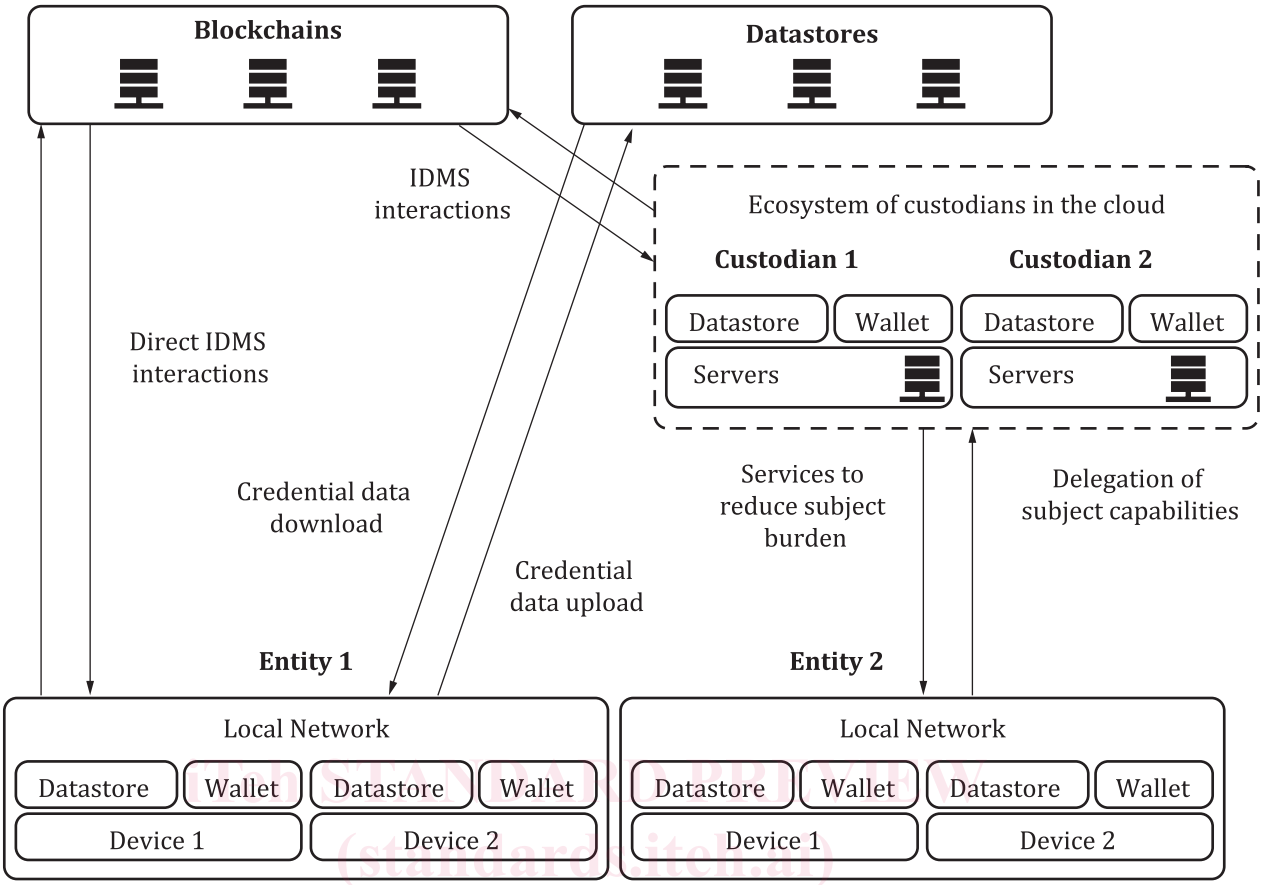

Figure 2 — Interactions between relevant actors

Users who lose their private keys can recover them if a specific key recovery mechanism has been put in place, such as a user-designated Custodian, a list of user-appointed trustees (social recovery), time delay mechanisms and/or a central authority (when suited). Custodians could offer their services through a competitive market. Some types of credentials can be transferrable from one user to another, as when they represent ownerships relations. All these interactions could be delegated through Custodians.

From one or more credentials it is possible to derive a presentation that allows Subjects to share verifiable information directly with a relying party and authenticate themselves. This presentation disclosure could be selective when it includes just a minimal amount of information, on a need-to-know basis, thanks to advanced cryptographic techniques such as zero-knowledge proof (in this context, presentation means information derived from one or more credentials that a subject discloses to a verifier to communicate some quality about a subject).

Users can be able to maintain a set of special purpose identifiers not linked with their primary identifier, e.g. by using pairwise pseudonymous identifiers with a dedicated identifier for each relationship with a third-party. A pairwise pseudonymous identifier is an opaque unguessable subscriber identifier generated by a Credential Service Provider (CSP) for use by a specific individual Relying Party (RP). This identifier is only known to and only used by one CSP-RP pair. See https://csrc.nist.gov/glossary/term/Pairwise_Pseudonymous_Identifier

5.2.4 Identifier origination schemes

The identifier origination schemes introduced before could be implemented in different ways, including:

— Credential Registry Acting as Identifier: the credentials for each participant in the system are stored in a smart contract deployed on the system. This is typical of bottom-up approaches. Standards such as ERC-725, Proxy Account, alleviate the burden on the blockchain from the need to deploy a smart

contract for each new identity in the system, and ERC-725 Key Manager, allows subjects to delegate certain capabilities to custodians.

— Global Identifiers Registry: a single monolithic (set of) smart contract(s) that acts as a global registry for storing and managing all identifiers. The smart contract(s) logic defines the different governance models. The registry can contain all the logic and data to resolve identifiers to their metadata or hashes to the actual data stored elsewhere.

— Anchors Registry: A single monolithic smart contract that acts as a global registry. The registry contains hashes of identifier management operations that are grouped together into bundles or anchors. The bundling is executed by a second level layer protocol, with the help of some decentralized storage.

— Bring-Your-Own Blockchain Address: there is no need to register an identifier before using it, and any blockchain address is a valid identifier. The main difference from the approaches based on smart contracts is that identifiers are not initially registered and stored on-chain, so they are non-discoverable.

— Unspent Transaction Output Model: this is the identifier scheme used in Bitcoin and other cryptocurrencies, where identifiers are created by submitting transactions to the blockchain, as recipients of the unspent output from a transaction.

5.2.5 Credential architectures

Credentials could be stored on-chain or off-chain. On-chain credentials could be implemented such that only the hashes of the credentials are stored on the blockchain, for comparison purposes. Different credential architectures are possible including:

— Per-Identifier Credentials Registry: Credentials are managed as entries in a per-identifier smart contract that acts as a container. The subjects could have unilateral control over their credentials, adding or removing them from the contract as preferred. This architecture creates a significant load on the blockchain. ERC-735, Claim Holder, reduces the burden on the blockchain.

— Global Credentials Registry: In this case, there is a single smart contract. The identifier that has deployed the system owns this smart contract, and could delegate, transfer, or limit the authority over it with respect to other identifiers: this architecture supports credentials revocation. Examples of this architecture are ERC-780, Ethereum Claims Registry and ERC-1056.

— Non-Fungible Token Repository: in this approach a Credential is a Non-Fungible Token (NFT), a token that is unique and possibly transferable. NFT Repositories are useful for managing digital ownership. Example of this architecture are ERC-721, Non-fungible Token Standard.

— User-Mintable, Predefined, Non-Fungible Token: in this architecture a credential takes the form of an entitlement to let a user create ("mint") a predefined and pre-assigned NFT according to specific conditions.

— Off-chain Object: in this architecture, a credential is an off-chain object, that manages the direct communication between parties.

Architectures for identifiers as in 5.2.4 could be combined with different architecture credentials, with possible examples:

— Global Identifiers Registry and Per-Identifier Credentials Registry: SmartID project from Deloitte.

— Global Registry for Identifiers and for Credentials: Smart contract-based PKI (SCPKI), BlockPKI.

— Off-chain Objects with Global Credentials Registry: uPort, Hyperledger Indy.

— Non-fungible Tokens with Global Credentials Registry: ERC-1616, Attribute Registry.

5.3 Functional role of DLT in identity systems

Different initiatives propose different roles for the DLT in identity management. Most popular roles include:

— Associating identifiers with public keys ("Decentralized PKI"): within this role, a DLT is primarily used for establishing an association between an identifier and a public key.

— Attestation of credentials: similar to digital signature or timestamping on credential as found in traditional systems.

— Support for credentials revocation: the DLT is used to support the revocation of credentials.

— Definition of common credential templates: a common template for credentials is stored in the DLT, to promote interoperability.

— Trust Anchors: DLT can be used to define some initial trust anchors.

5.4 Trust Over IP Foundation

The Trust over IP (ToIP) Foundation (https://trustoverip.org/), homed at The Linux Foundation, aims to simplify and standardize how trust is established online so that everyone can feel safe, secure, and private in all of our digital interactions—whether between individuals, businesses, governments, or any "thing" on the Internet of Things.

Its mission is to define a complete architecture for Internet-scale digital trust that combines cryptographic trust at the machine layer with human trust at the business, legal, and social layers, specifying how standards and components can be combined to fulfil the requirements of all four layers of the stack, for both governance and technology.

6 Existing DLT systems for identity management

6.1 General

This clause contains a list of examples that includes (but it is not limited to) several relevant existing systems.

6.2 uPort

uPort[1)] [7], provides a platform for self-sovereign digital identity management (Self-Sovereign Identity is an emerging concept associated with the way identity is managed in the digital world. According to the Self-Sovereign Identity approach, users are expected to be able to create and control their own identity, without relying on any centralized authority, see https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf). The provided platform includes:

— The uPort Serto App, to re-forge user trust by putting users back in control of their personal data and identity. With the uPort app they can locally store their credentials and decide when and with whom they want to share.

— The uPort SDK, to integrate uPort's trusted data and identity management platform solution in a mobile app, letting customers securely store their private data with confidence and peace of mind. They can control their most important attributes and how and when they share them with companies, institutions, and peers.

— The uPort Libraries.

1) uPort is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.