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

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.

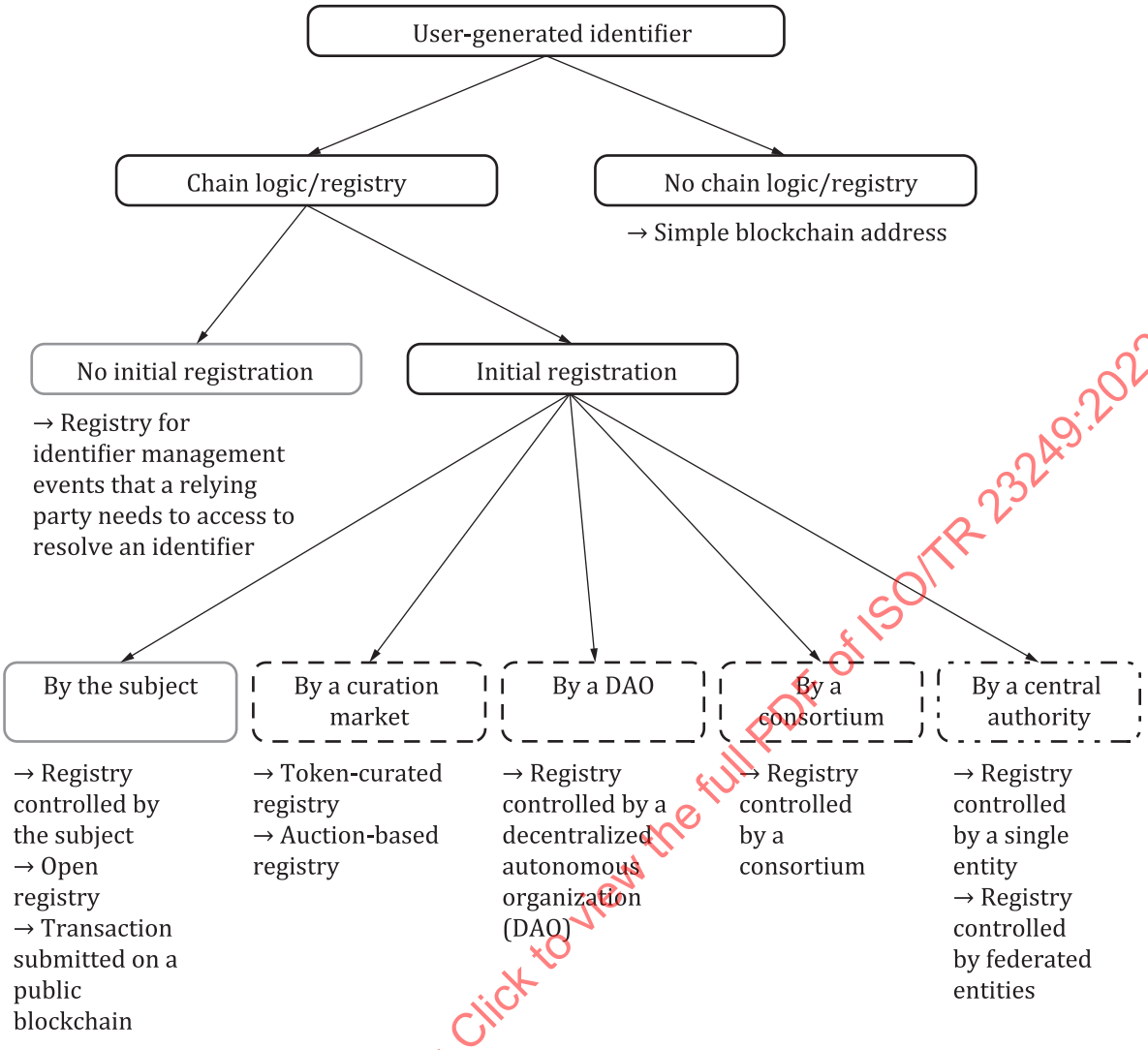


Figure 1 — Identifier origination schemes

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).

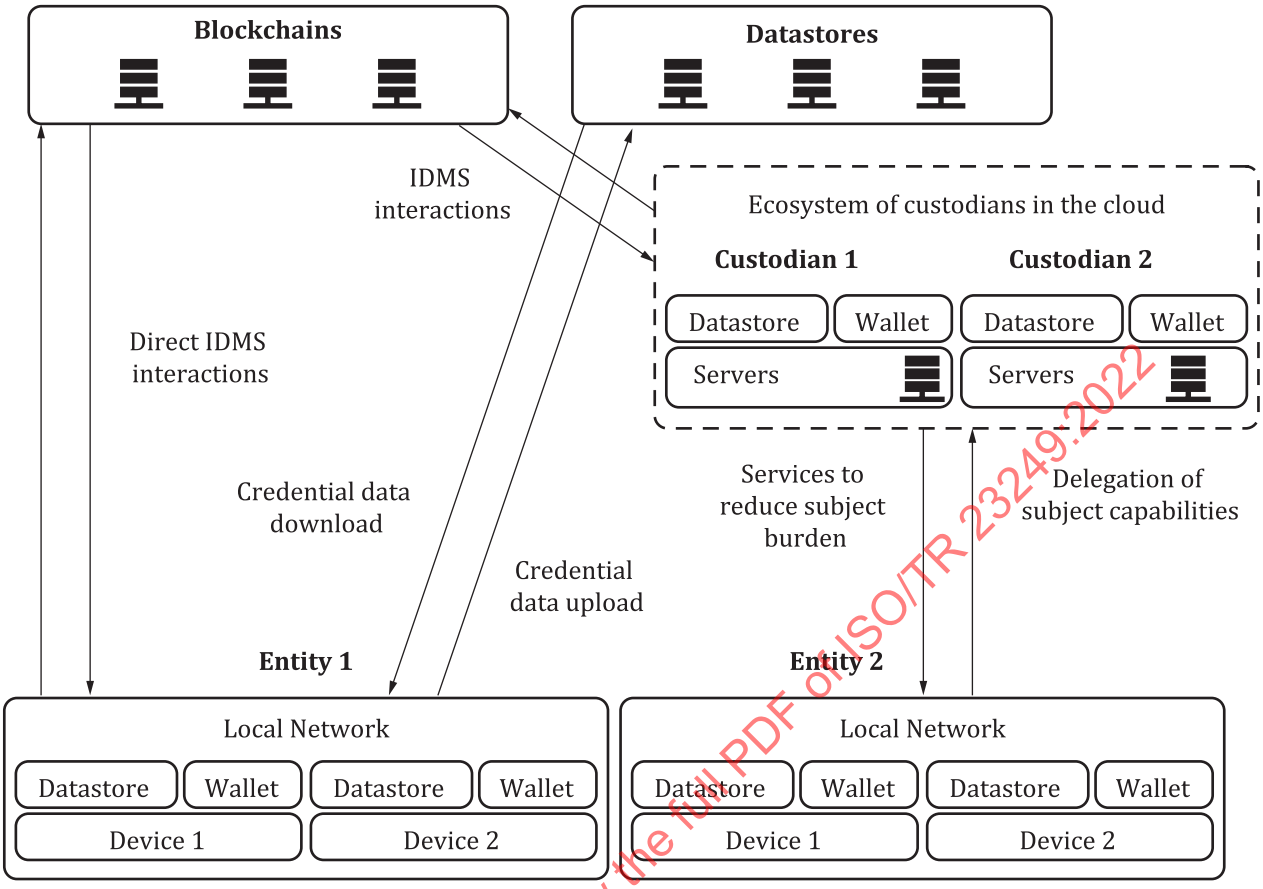


Figure 2 — Interactions between relevant actors

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.

uPort is described as a self-sovereign digital identity platform – anchored on the Ethereum blockchain. The uPort technology primarily consists of smart contracts, developer libraries, and a mobile app. uPort identities are fully owned and controlled by the creator – independent of centralized third-parties for creation, control or validation.

The company offers a collection of tools and protocols for building decentralized user-centric applications, built on open standards and open source libraries. It is based in the use of Ethereum addresses as identifiers and the use of a specific contract for registering and managing DIDs, according to the ERC-1056 Lightweight Identity Ethereum Improvement Proposal (EIP), and JSON Web Tokens for protocol requests and responses, according to IETF RFC 7519 (https://tools.ietf.org/html/rfc7519).

As explained in the uPort specifications, a uPort identity is just someone or something that can sign data or transactions and receiving signed data about itself.

An identity has:

— An Identifier in the form of a DID.

— A signing key.

— A public key stored on the uPort Registry.

uPort[8] provides an Ethr-DID library conforming to ERC-1056 intended to use Ethereum addresses as fully self-managed DIDs. It allows a user to easily create and manage keys for these identities and lets the user sign standards compliant JSON Web Tokens (JWT) that can be consumed using the DID-JWT library. This library encapsulates the functionality of Ethr-DID-Resolver and Ethr-DID-Registry, and supports the following capabilities:

— Create and manage keys for DID identities.

— Sign JWTs.

— Authorize third parties to sign on a DID's behalf.

— Enable discovery of service endpoints (e.g. decentralized identity management services).

The Ethr-DID-Registry is a smart contract that facilitates public key resolution for off-chain (and on-chain) authentication. It also facilitates key rotation, delegate assignment and revocation to allow 3rd party signers on a key's behalf, as well as setting and revoking off-chain attribute data. These interactions and events are used in aggregate to form a DID's DID document using the Ethr-Did-Resolver.

The Ethr-DID-Registry supports the following operations:

— Looking up identity ownership.

— Changing identity ownership.

— Looking up a delegate.

— Adding a delegate. Delegates are needed to allow Web3 providers to sign a change identity owner operation or to sign JWTs (a Web3 provider is the way the Web3.js framework talks to the blockchain, see https://web3.py.readthedocs.io/en/stable/providers.html)

— Revoking a delegate.

— Enumerating delegates off-chain.

— Setting off-chain attributes.

— Revoking off-chain attributes.

— Reading off-chain attributes.

— Enumerating linked identity events.

— Assembling a DID document.

An identity can:

— Sign JWTs to authenticate themselves to a third party, and disclose private information about themselves.

— Receive requests for disclosure about themselves.

— Receive and store signed third party verifications about themselves.

— Sign Ethereum transactions.

Currently, uPort supports the following application flows[9]:

— Send Verification Claim Flow, to allow a user to request a Verified Claim to an issuer, and an issuer to create and deliver Verified Claims to a user. A Verifiable Claim is always signed by the issuer, and includes the DID of the issuer, the DID of the subject, the time of issuance and a set of one or more claims.

  Different claims about the same entity will have the same subject DID, essentially corresponding to her Ethereum address, allowing linkability [from an attacker's perspective, the linkability of two or more items of interest (IOIs), e.g., subjects, messages, actions, ... means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not, see https://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html]. Conversely, unlinkability is the inability for the attacker to sufficiently distinguish whether these IOIs are related or not.

— Selective Disclosure Flow, to allow a relying party to request a user for claims. This flow is formed by a Selective Disclosure Request and a Selective Disclosure Response. The Selective Disclosure Request can specify requirements for claims (based on the OpenID-Connect specification adapted to support Verifiable Claims) requested from a user. The response is always signed and it normally includes an array of Verified Claims JWTs or IPFS hash of JSON encoded equivalent.

— Ethereum Transaction Request Flow, to allow a client application request a user to sign an Ethereum transaction.

— Private Chain Provisioning Flow, with experimental support for supporting Ethereum accounts on private chains.

6.3 Decentralized Identity Foundation (DIF)

DIF (https://identity.foundation/) is an engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interoperability between all participants.

DIF focuses in developing specifications and emerging standards for protocols, components, and data formats that implementers can execute against, and seeks to align industry participants to advance their common interests.

Currently DIF has the following working groups:

— Identifiers and discovery.

— Storage and compute.

— Authentication.

— Claims and credentials.

— DID Communication.

— Sidetree development & operating group.

— Secure data storage.

— Interoperability.

DIF produces the following specifications related to this document:

— Universal Resolver: specification and implementation of a driver-based framework that enables resolution of DIDs.

— Universal Registrar: specification and implementation of a driver-based framework that enables creation/updates/deactivation of DIDs.

— Well-known DID configuration: specifications, documents, and implementations for discovering DIDs from well-known HTTP(S) URIs.

— Identity Hubs: encrypted personal datastore for identity interactions and decentralized apps.

— DID Authentication Profile for SIOP: Defines how to use OpenID Connect (OIDC) together with the strong decentralization, privacy and security guarantees of DID for everyone who wants to have a generic way to integrate SSI wallets into their web applications.

— DIDComm JS Lib: A shared effort with the Hyperledger Aries project to create a standardized means of authenticated general message passing between DID controllers.

— Credential Manifest: The DID Credential Manifest is a format that aims to normalize the process of credential acquisition, wherein the issuer is able to describe the requirements that the subject or participant in the credential generation process needs to meet for the issuer to generate the desired credential.

— VC JSON Schemas: The VC JSON Schema specification aims to provide a standardized mechanism to use JSON Schemas as the data backing for Verifiable Credentials. Though the repository lives in the W3C-CCG, this working group contains key contributors and has a vested interest in contributing to the development of the specification.

— Sidetree protocol: specifications, documents, and implementations for the chain/ledger-agnostic DID scaling protocol.

6.4 Alastria ID

Alastria ID is the digital identity project of the Identity Commission of Alastria (https://alastria.io/), whose ecosystem in shown in Figure 3. Their proposal for digital identity in blockchain aims to provide an infrastructure and development framework, to carry out sovereign digital identity projects, with full legal validity in the euro zone, following these premises:

— Follow the guidelines of the e-Identity workshop report, of the EU Blockchain Observatory and Forum (https://www.eublockchainforum.eu/sites/default/files/reports/workshop_5_report_-_e-identity.pdf).

— Compliance with eIDAS Regulation.

— Make the digital identity in blockchain and the GDPR two complementary tools, following the recommendations described in EU Blockchain Observatory and Forum (https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf) and the study from European Parliamentary Research Service (https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU%282019%29634445_EN.pdf).

A digital identity[10] allows the user/subject to authenticate and present (certified) personal information in order to get a service, those actions require the creation and set-up of a digital identity and the gathering of certified personal information (credentials) from trusted sources.

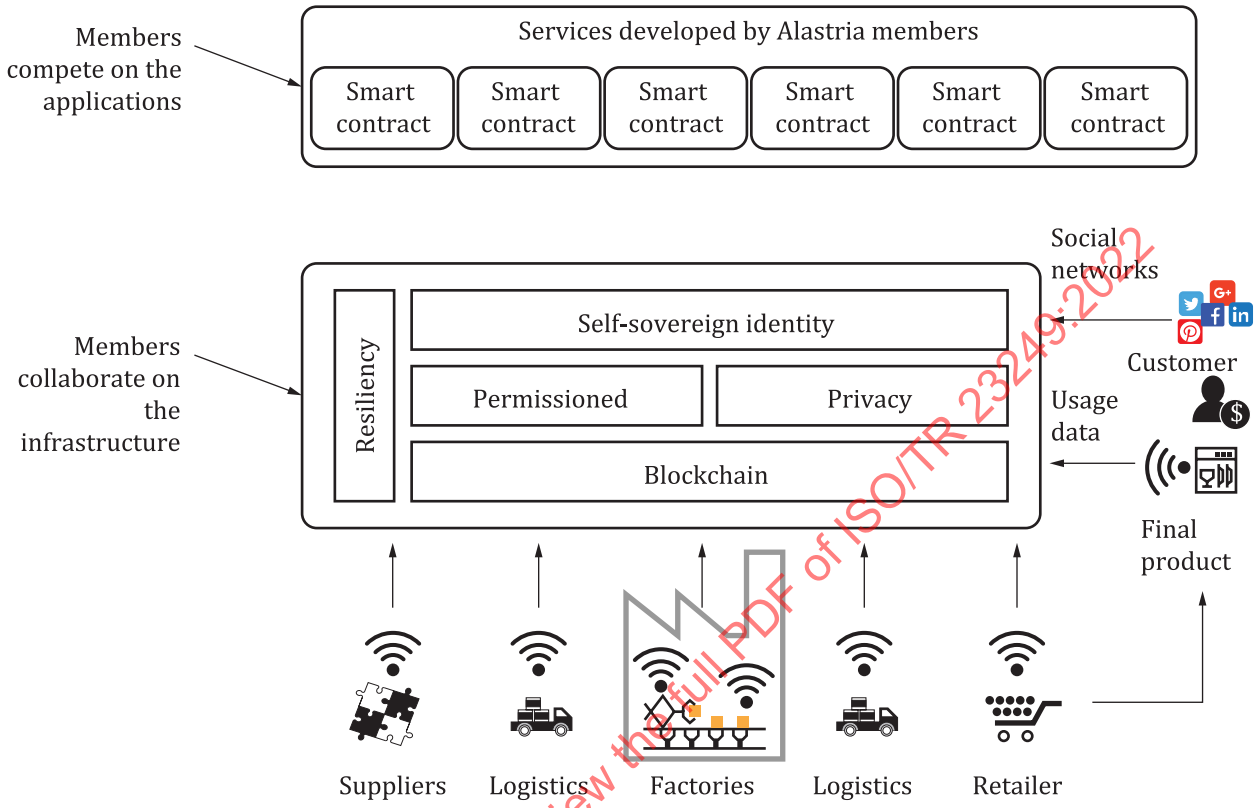


Figure 3 — Alastria ecosystem

For pseudonymous single usage, i.e. presenting some information in order to get a service where the service provider does not need to record anything and is not going to provide services in a recurrent way an Alastria ID is enough. Consider for example a user presenting a credential entitling to obtain a digital asset (photo, song, etc.) or access to a given place (building, conference centre).

When authentication is required or when recurrent service is going to be provided or when the service provider needs to record the presentation gathered, the Alastria ID could be recorded in order to make easier to provide the service or record interactions with the user.

For credential issuance linked to an Alastria ID, the Alastria ID also needs to be recorded by the entity.

Then, to use Alastria ID in front of a given entity (service provider or credential issuer) the user Alastria ID is likely to be recorded by the entity. When there is another identifier used by the entity to identify internally the same user (Legacy Id), the Alastria ID and the Legacy Id are intended to be linked together. The general flow of operations is shown in Figure 4.

There are different situations that are possible for the relationship between a subject and a given entity (service provider or credential issuer), depending on whether the user has an Alastria ID, a Legacy Id for that entity and whether the Alastria ID is recorded (and linked to the Legacy Id) by the entity.

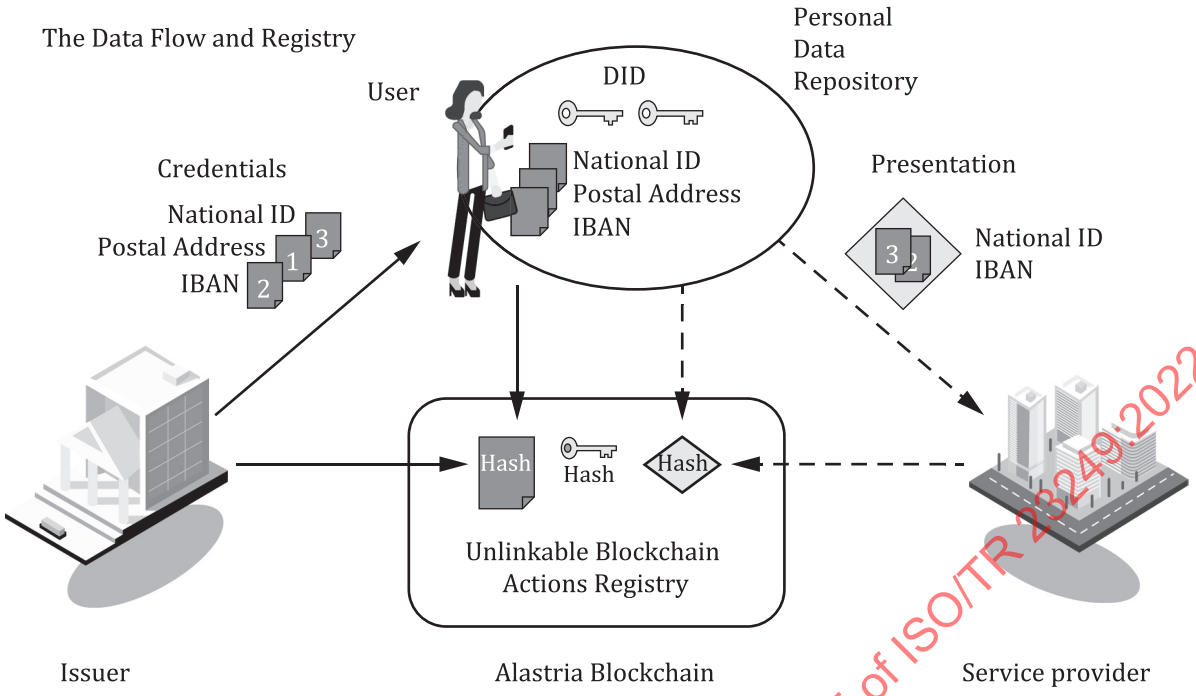


Figure 4 — General view of Alastria ID flows and registry

Alastria ID considers the following operations:

— Alastria ID creation. Subjects are identified by DIDs anchored in an Ethereum network, as in the uPort/DIF initiatives.

— Onboarding with Alastria ID.

— Alastria ID registration & legacy Id linking.

— Alastria ID authentication.

— Alastria ID credentials: credential issuance, credential revocation, credential query status.

— Alastria ID presentations: present presentation, withdraw presentation, presentation query status.

Credential issuance and presentation operations are registered in the DLT as evidence. Each credential operation generates a specific hash, that stored in a tuple associated with the corresponding role. To avoid correlation, the issuer generated credential hash and the user generated credential hash are different. Similarly, the user generated presentation hash and the relying party generated presentation hash are also different. See Figure 5 for a pictorial representation.

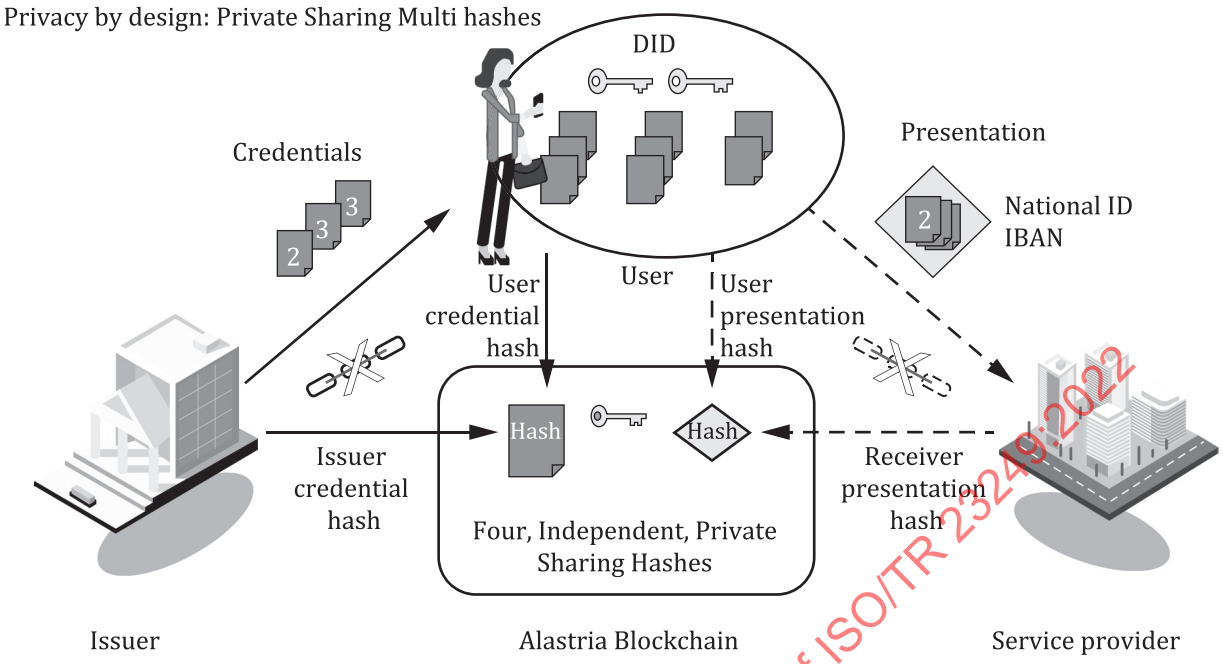


Figure 5 — Unlinkability of transactions

6.5 European Self Sovereign Identity Framework (ESSIF)

The European Blockchain Services Infrastructure (EBSI, see https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI) is a joint initiative from the European Commission and the European Blockchain Partnership (EBP, see https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership) to deliver EU-wide cross-border public services using blockchain technology. The EBSI is materialized as a network of distributed nodes across Europe (the blockchain), leveraging an increasing number of applications focused on specific use cases. In 2020, EBSI became a CEF Building Block, providing reusable software, specifications, and services to support adoption by EU institutions and European public administrations.

EBSI Platform is a peer to peer network of interconnected nodes. The European Commission operates a minimum number of EBSI nodes at European level and the Member States operate EBSI nodes at a national level. All the nodes are able to create and broadcast transactions that will update the ledger. The architecture of each node is composed of two main functional areas (see Figure 6, reproduced with permission from EBSI):

— A set of four layers comprising components which together provide the EBSI infrastructure, which contain capabilities common to all use cases. These layers include generic capabilities and connectivity to Blockchain networks.

— A set of two layers comprising use case-specific components enabling support for hosting of business applications.

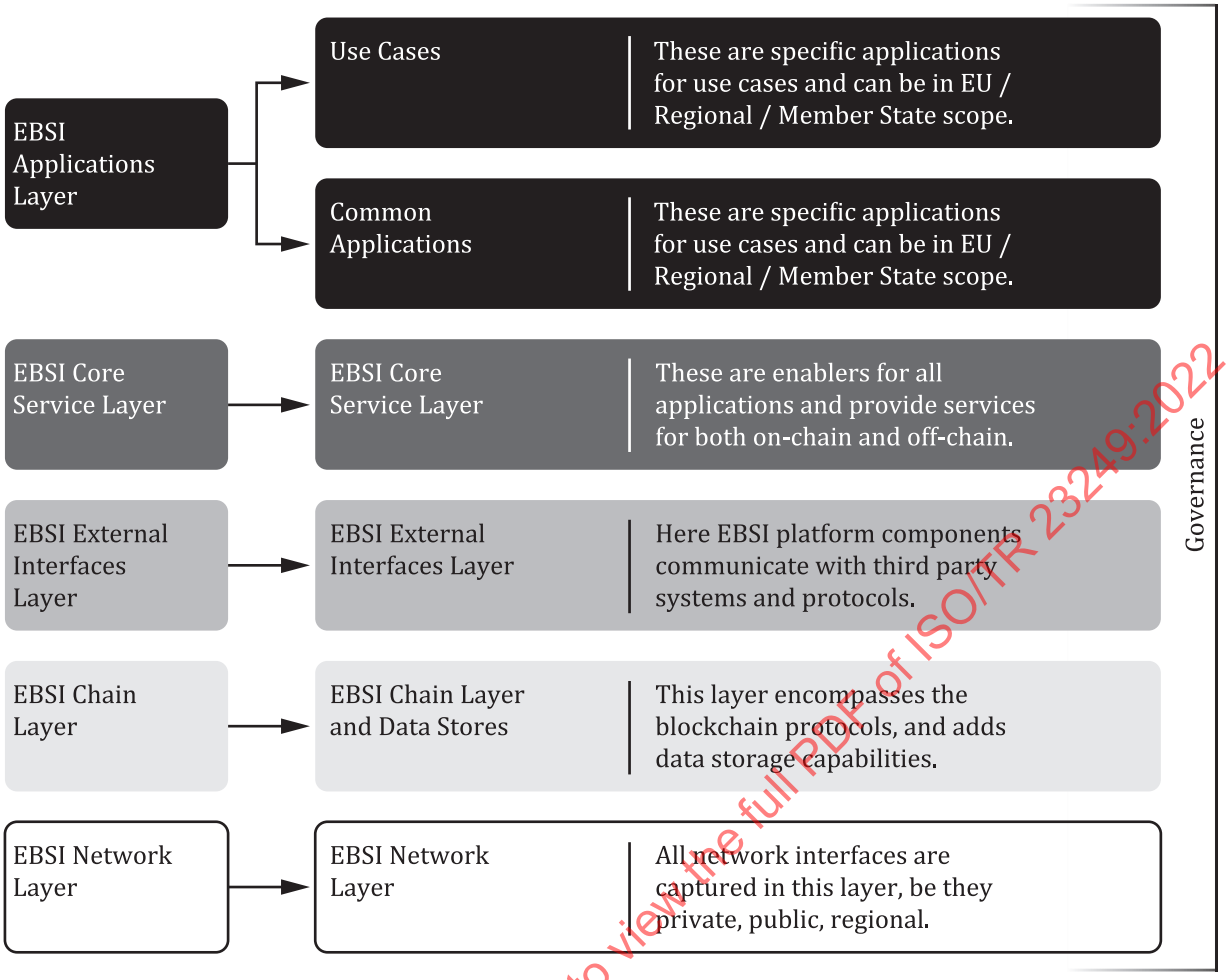


Figure 6 — EBSI layered approach

ESSIF is one of the use cases of EBSI, aiming to implement a generic self-sovereign identity (SSI) capability, allowing users to create and control their own identity across borders without relying on centralized authorities.

ESSIF has defined a data model considering:

— Identities and DIDs anchored in a DLT, allowing for multiple DIDs, aligned with W3C DID specifications.

— Verifiable IDs, a specific type of credential tailored for identification purposes under the current eIDAS Regulation.

— Verifiable Attestations, covering other credential types, when needed inheriting attributes from parent Verifiable IDs.

— Links with the eIDAS Levels of Assurance, and with the legal value of presentations.

ESSIF's key flows include:

— DID registration.

— Obtaining verifiable IDs.

— Obtaining verifiable attestations.

— Linking verifiable IDs with OpenID Connect.

— Submitting verifiable attestations.

Some of the specific components analysed include the eIDAS Bridge, to seal verifiable credentials, and the Trusted Issuers' Ledger. Figure 7 (reproduced with permission from EBSI) shows the different user stories for the different actors in the system.

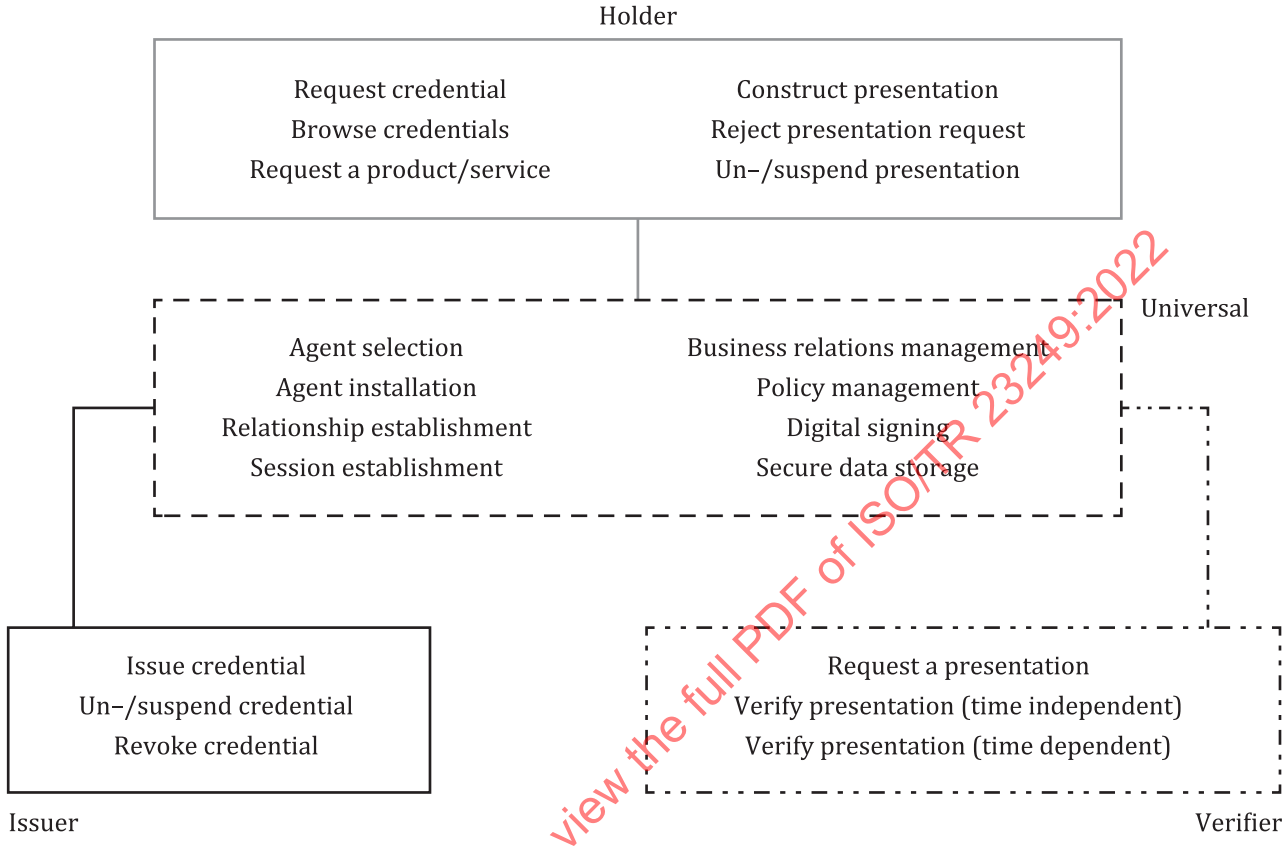


Figure 7 — ESSIF User stories per actor

6.6 Sovrin™ Network, Hyperledger Indy, Hyperledger Aries and Hyperledger Ursa

The Sovrin™[2] Network (https://sovrin.org/) is described as a public service utility enabling self-sovereign identity on the Internet. The Sovrin Network is decentralized, meaning individuals can collect, hold, and choose which identity credentials –such as a driver's license or employment credential– without relying on individual siloed databases that manage the access to those credentials.

Sovrin™is an open source project that offers the tools and libraries to create private and secure data management solutions that then run on the identity network of Sovrin™.

The following is the set of actors who play a role in the Sovrin™ Network (see Figure 8 and Figure 9):

— Holder/Prover: acquires, stores and presents identity claims to an inspector, and submits a registry identifier to the identifier registry.

— Issuer: issues identity claims to a holder and verifies identifier ownership through the identifier registry.

— Inspector/Verifier: requests claims from holders and verifies identifier ownership through the identifier registry.

— Identifier registry: in charge of maintaining the digital identifiers (DID's) registered.

2) Sovrin is the trademark of a product supplied by the Sovrin Foundation. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

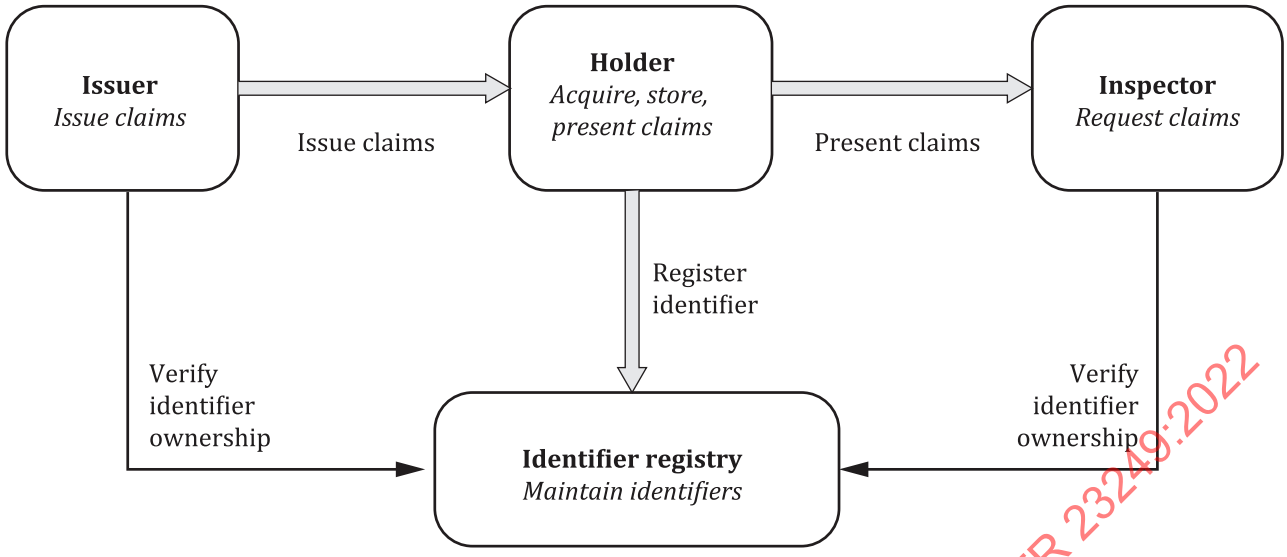
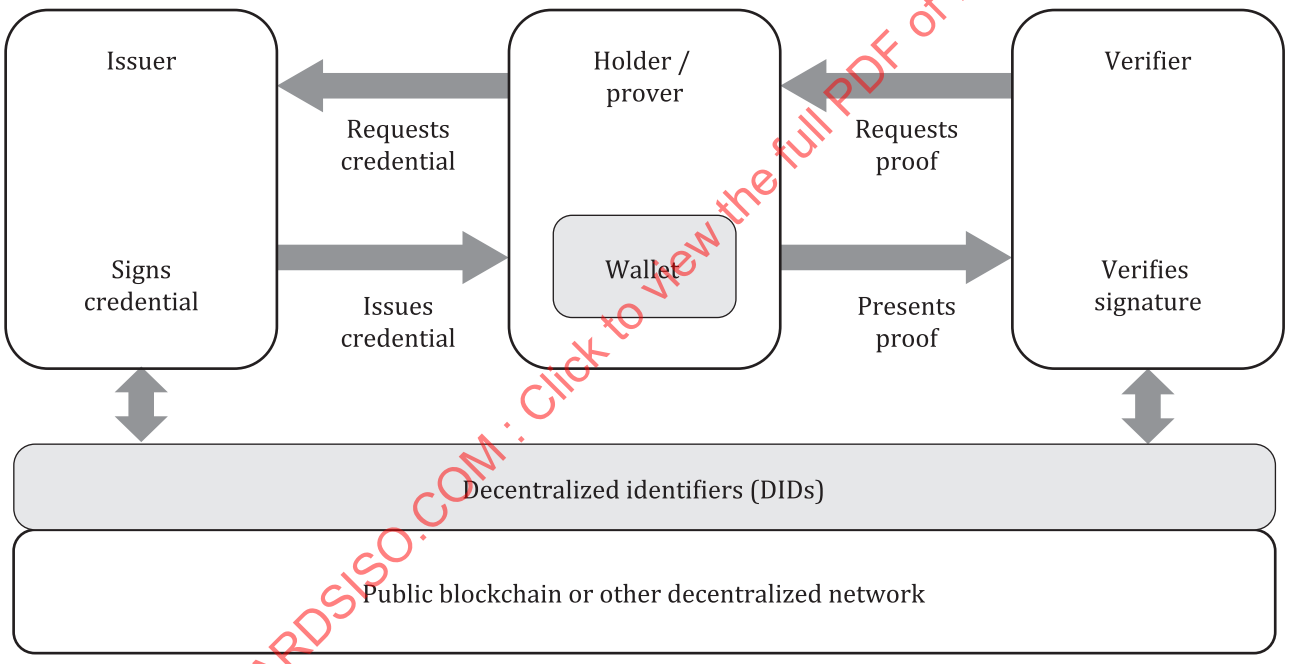


Figure 8 — General roles (similar to W3C Verifiable Credentials Data Model)



NOTE Reproduced with permission from ssimetup.org.

Figure 9 — Roles and main flows instantiation

Sovrin™ is a consortium blockchain where everybody can use the platform, without prior permission. However, Sovrin™ is permissioned ledger with a known set of validator nodes, called stewards, which achieve consensus on the ledger.

Sovrin™ uses DKMS, a new approach to cryptographic key management intended for use with blockchain and distributed ledger technologies (DLTs) where there are no centralized authorities[11]. DKMS inverts a core assumption of conventional PKI (public key infrastructure) architecture, namely that public key certificates will be issued by centralized or federated certificate authorities (CAs). With DKMS, the initial "root of trust" for all participants is any distributed ledger that supports a new form of root identity record called a DID.

A DID is a globally unique identifier that is generated cryptographically and self-registered with the identity owner's choice of a DID-compatible distributed ledger, so no central registration authority is required. Each DID points to a DID document—a JSON or JSON-LD object containing the associated public verification key(s) and addresses of services such as off-ledger agent(s) supporting secure peer-to-peer interactions with the identity owner.

DIDs are a new type of identifier designed for cryptographically verifiable digital identity that are "independent" or "self-sovereign", i.e., fully under the control of the identity holder and not dependent on any centralized registry, identity provider, or certificate authority.

A DID added directly to the Sovrin™ public ledger is called a public DID, whereas a pairwise pseudonymous DID shared and stored privately "off-ledger" between the agents for two identity holders is called a private DID. The ability for Sovrin™ infrastructure to support both is fundamental to both its Privacy by Design architecture as well as its ability to scale.

Since no third party is involved in the initial registration of a DID and DID document, it begins as "trustless". From this starting point, trust between DID-identified peers can be built up through the exchange of verifiable credentials—credentials about identity attributes that include cryptographic proof of authenticity of authorship.

Sovrin™ identity holders can also choose to have one or more DIDs and associated DID documents added to the Sovrin™ public ledger.

In Sovrin™ Infrastructure, the DKMS standard applies to Wallets and Agents. A Wallet can be defined as a software module, and optionally an associated hardware module, for securely storing and accessing Private Keys, Link Secrets, other sensitive cryptographic key material, and other Private Data used by an Entity. A Wallet is accessed by an Agent. An Agent is a software program or process used by or acting on behalf of an Entity to interact with other Agents or with the Sovrin™ Ledger or other distributed ledgers. Agents are of two types: Edge Agents run at the edge of the network on a local device; Cloud Agents run remotely on a server or cloud hosting service. Agents require access to a Wallet in order to perform cryptographic operations on behalf of the Entity they represent.

The Sovrin™ architecture is summarized in three layers:

— Sovrin™ Ledger: is the key component of Sovrin™ project. It is a distributed ledger of non-profit public organizations governed by Sovrin™ Foundation. The steward nodes of this ledger run The Plenum protocol, which is an enhancement version of the redundant Byzantine fault tolerant protocol.

— Sovrin™ Agents: Users interact with Sovrin™ through agents that are acting as addressable network end points. Sovrin™ agents provide many functions in the network such as Persistent P2P messaging endpoints, coordination endpoints for multiple clients, encrypted data storage and sharing, etc.

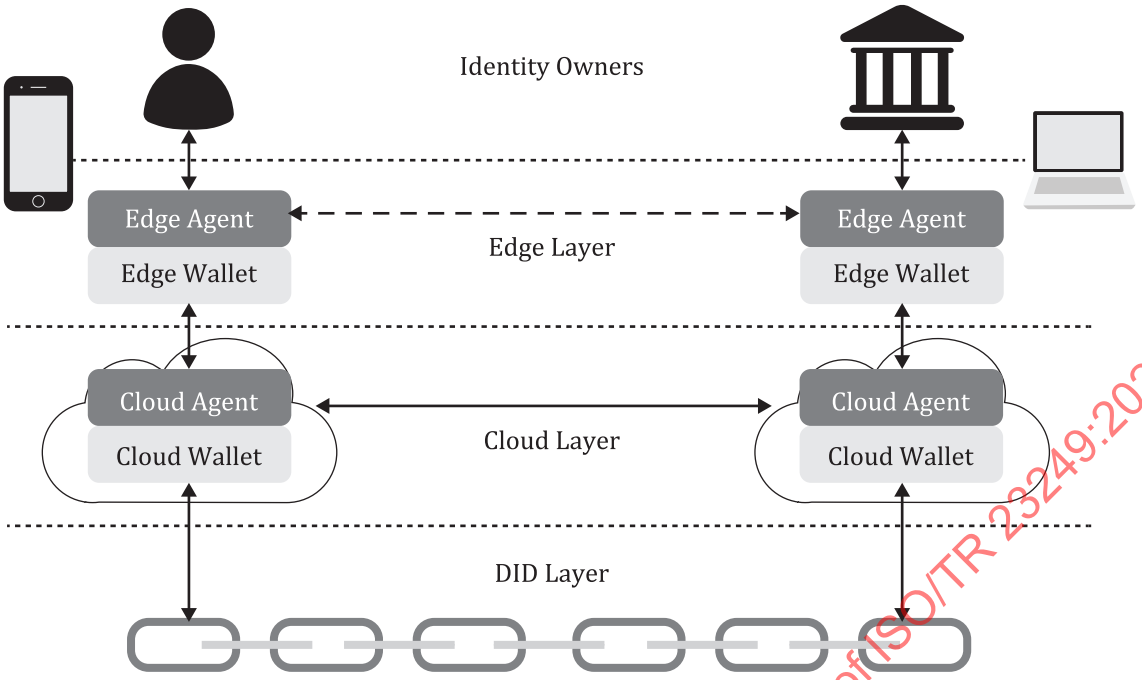
— Sovrin™ Clients: Applications operated on edge devices (smartphone, laptop, etc.) to ensure the communication with Sovrin™ agents and ledger in order to conduct identity transactions.

At a high level, the corresponding abstract DKMS architecture consists of three logical layers see Figure 10):

— The DID layer is the foundational layer consisting of DIDs registered and resolved via distributed ledgers.

— The cloud layer consists of server-side agents and wallets that provide a means of communicating and mediating between the DID layer and the edge layer. This layer enables encrypted peer-to-peer communications for exchange and verification of DIDs, public keys, and verifiable credentials.

— The edge layer consists of the local devices, agents, and wallets used directly by identity owners to generate and store most private keys and perform most key management operations.



NOTE Reproduced with permission from ssimetup.org.

Figure 10 — DKMS layered abstract approach

Sovrin™ architecture supports five basic claim types. All of them store claims data as JSON objects, the standard data interoperability format for Sovrin™:

— Cleartext claims are directly readable, with no hashing or encryption. Public cleartext claims are intended for public identities with no expectation of privacy, e.g., claims about business and governmental identities that are a matter of public record (and which with Sovrin™ can be fully verified).

— Encrypted claims contain an encrypted version of a cleartext claim, where the entire claim can be decrypted with a single symmetric or asymmetric private key.

— Hash signature claims contain a specially encrypted tree of cleartext claims, where the identity owner can selectively reveal specific claims to specific relying parties.

— Proof of existence claims (aka POE claims or hash claims) are simply hashes of digital objects that enable an identity owner to prove that a digital object existed at a point in time. POE claims are especially useful for proving consent as required under privacy regulations such as the EU General Data Protection Regulation (GDPR). When an identity owner gives consent to a relying party for a particular usage of personal data under GDPR, a hash of the consent receipt or link contract to which both parties agreed can be written to the ledger as a claim. The hash itself does not reveal any information about the consent—or even the relationship of the parties— but can be used by either party to prove consent was granted.

— Anonymous credentials transmit claims information without actually containing either a cleartext or encrypted version of the claims data. Rather they are a cryptographic method of providing a proof about a claim. The classic example of an anonymous credential is a proof of age (i.e. “over 21”) that does not reveal the actual birthdate.

Using Sovrin™, an inspector/relying party can, for the first time, do all of the following without ever needing to contact the issuer of a credential:

— Confirm that the data provided to them (or proofs about such data) by an identity holder came from the stated issuer.

— Confirm that the data is unchanged.

— Confirm that the data was provided only to the identity holder who has presented it.

— Confirm that the data has not been revoked by the issuer.

Also, an issuer can:

— Create and issue any type of credential without waiting for a central body or data hub to update its limited transaction set to accommodate it.

— Revoke credentials that it issues, without needing to create complex and privacy-leaking user experiences or handle multiple technical integrations with thousands or millions of relying parties.

— Provide its customers with trustworthy digital credentials that can be used anywhere in the world instantly.

— Revoke the ability of a lost/stolen device to be used to fraudulently represent the identity holder.

And all of the above can be done in a highly privacy-preserving manner, protecting the identity holder from intended or unintended correlation and inadvertent data leakage.

Finally, the elements stored on the Sovrin™ distributed ledger include:

— Public DIDs and associated DID documents with verification keys and endpoints (defined above).

— Schemas and credential definitions: To support the interoperable exchange of verifiable credentials, the Sovrin™ ledger stores two specific objects: schema definitions and credential definitions.

  A schema definition is a machine-readable definition of a set of attribute data types and formats that can be used for the claims on a credential. Once a schema definition has been written to the Sovrin™ ledger, it can be used by a credential issuer (bank, passport office, university, employer, etc.) to create an issuer-specific credential definition that is also written to the Sovrin™ ledger.

— Revocation registries: this is a new solution to credential revocation that is decentralized, asynchronous and private.

  A revocation registry is data structure written to the Sovrin™ ledger by the issuer. It references the credential definition and contains a single (long) number called a cryptographic accumulator. This number can be checked instantly by any relying party when it needs to ensure a data in a proof it has been given has not been revoked by the issuer.

— Agent authorization policies. This is another specialized use of cryptographic accumulators and zero-knowledge cryptography on the Sovrin™ ledger to enable an identity holder to prove to a relying party that a particular agent is authorized to communicate on the identity holder's behalf.

Elements that are never stored in the Sovrin™ distributed ledger include:

— Private DIDs.

— Private credentials.

— Consent receipts or records of credential exchange transaction.

The Sovrin™ protocols has been donated and is maintained by the Hyperledger open source collaborative effort, as part of the Linux Foundation.

Hyperledger™[3] Indy (https://www.hyperledger.org/use/hyperledger-indy) provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed

3) Hyperledger is the trademark of a product supplied by the Hyperledger Foundation. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

ledgers so that they are interoperable across administrative domains, applications, and any other silo. Specifically, the Sovrin™ Network is the largest public deployment of Indy.

Hyperledger™ Aries (https://www.hyperledger.org/use/aries) is an infrastructure for blockchain-rooted, peer-to-peer interactions. It includes a shared cryptographic wallet for blockchain clients as well as a communications protocol for allowing off-ledger interaction between those clients. This project consumes the cryptographic support provided by Hyperledger Ursa (https://www.hyperledger.org/use/ursa), to provide secure secret management and decentralized key management functionality.

6.7 WEF Known Traveller Digital Identity (KTDI™)

The Known Traveller Digital Identity (https://ktdi.org/), is a World Economic Forum initiative that brings together a global consortium of individuals, governments, authorities and the travel industry to enhance security in world travel[12].

KTDI™[4)] allows individuals to manage their own profile and collect digital attestations of their personal data, deciding what data to share and when. The more attestations a traveller accumulates and shares, the better consortium partners, governments and other parties can provide a smooth and safe travel experience.

The following is the set of actors who play a role in the KTDI™ initiative:

— Travellers who want to benefit from the following:

  — Eliminating redundancy, specifically the need to fill out the same information when booking a flight, hotel, car, visa application, immigration card, fast-track programme, VAT recovery, etc.

  — Expedited passage since immigration, hotel check-in and others have complete, formatted customer identify and information.

  — Accelerated decision-making from governments regarding entry.

— Airlines whose benefits are:

  — Increased accuracy and reduced airline fines/exposure through valid identity management, such as a mobile passport passed via the platform.

  — Reduced distribution of customs forms to each flight allowing staff to serve customers.

  — Faster connections of travellers would allow airlines to reduce block times and still have as many connecting opportunities, perhaps leading to greater aircraft utilization.

  — Lowering landing costs and station rents by reallocating space at airports to retailers.

— Hotels that want to benefit from the following:

  — Improving service efficiency as front-desk representatives will not need to ask travellers for a passport, photocopy it, and file it, speeding up the check-in process, and improving safeguarding of customer data.

  — Ensuring accurate staffing at hotels through more accurate arrival/departure information.

— Airports that want to benefit from the following:

  — Freeing up space as customers have virtual forms filled out and do not require areas dedicated to fill out forms.

  — Improving airport and city perception as queues become smaller given that more people can be expedited.

4) KTDI is the trademark of a product supplied by the World Economic Forum. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

  - Lowering landing costs and station rents by reallocating space at airports to retailers.
- Governments that want to benefit from the following:
  - Ensuring data accuracy by exposing the data from the virtual hub/platform.
  - Guaranteeing complete data for profiling/risk purposes thanks to the platform, as passengers' book outside the global distribution system (GDS) channel 50 % to 70 % of the time.
  - Better decision-making thanks to more customer data; governments can spend more time on people without as much background data, which can make their countries safer.
  - Clearer traveller profiles could influence foreign governments' decision to allow entry and expedite admittance to Fast Track programmes or expedited lanes (knowing that a person is already a member of US Global Entry could give another country more confidence in expediting that person's entry).
  - Greener as there will not be the need to print as many forms and worry about their distribution.
  - More efficiency by having all of the data from the forms in a standardized, easy-to-read, already-input system and avoid storage of paper or scanning or data entry.
  - Reducing staffing and training costs as passengers can be scanned more efficiently resulting in agents handling more passengers.

Figure 11 to Figure 16 (from Reference[5]) show the steps of a practical use case involving most of the actors we have described above:

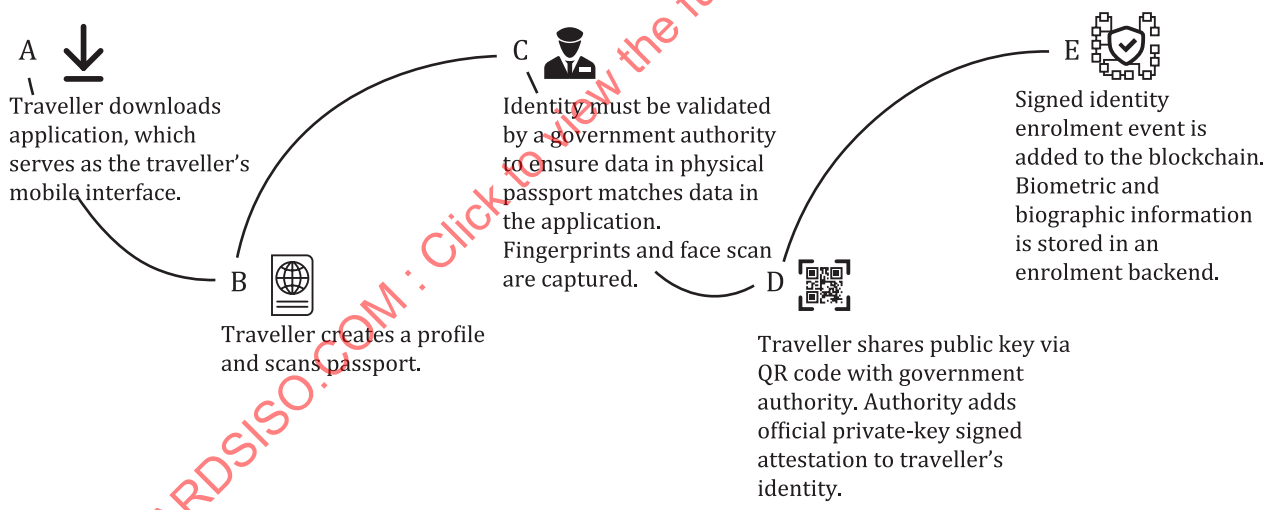


Figure 11 — Known Traveller Digital Identity enrolment

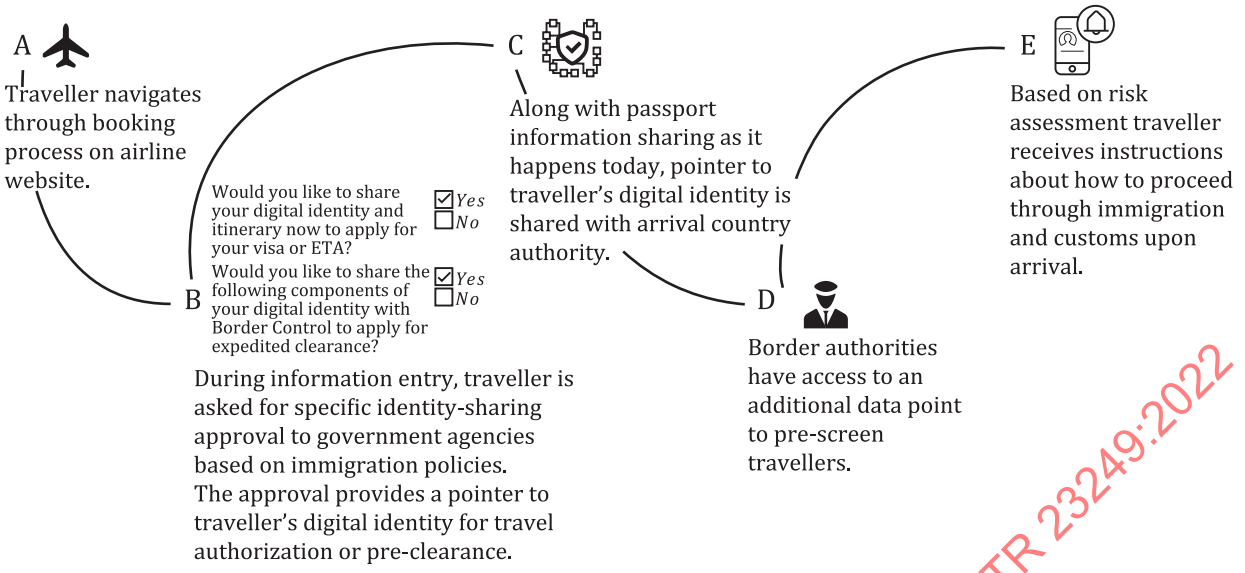


Figure 12 — Pre-trip: Booking, travel authorization and pre-screening

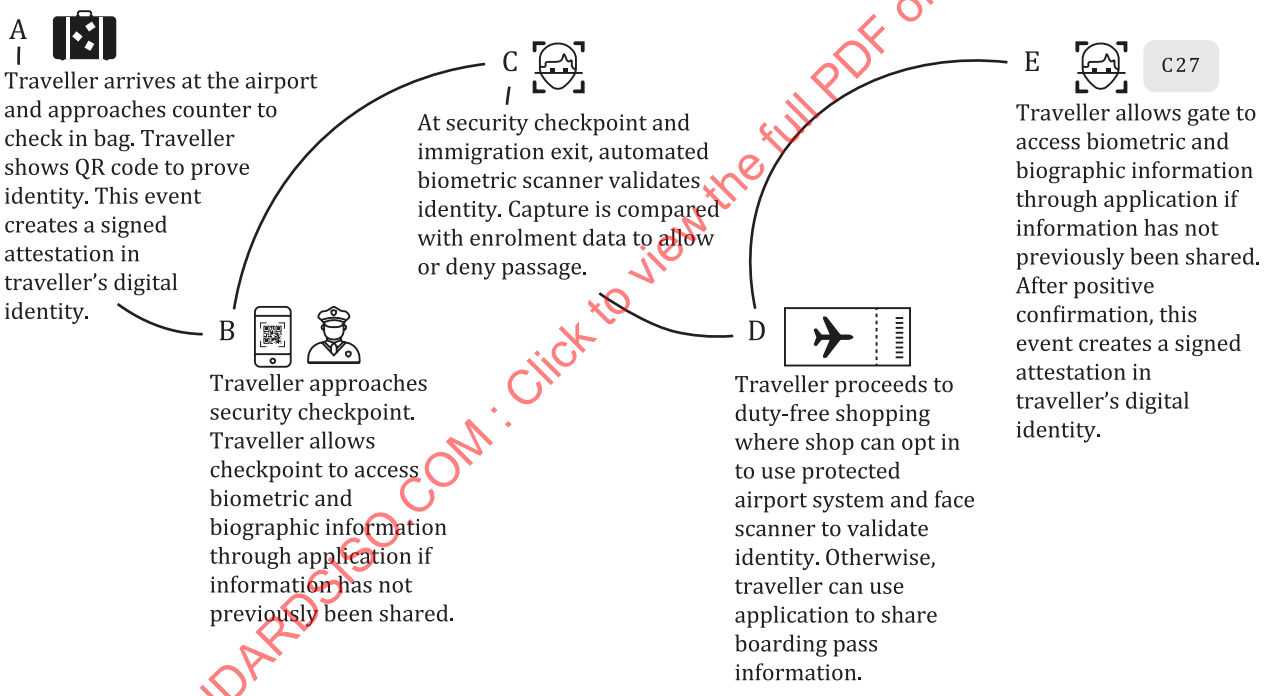


Figure 13 — Departure

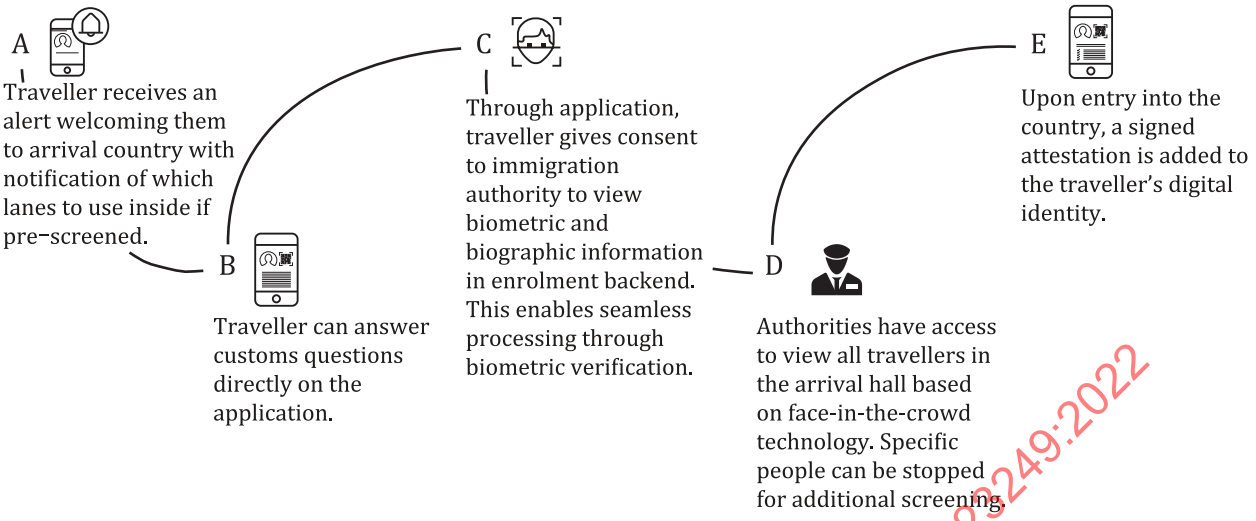


Figure 14 — Arrival

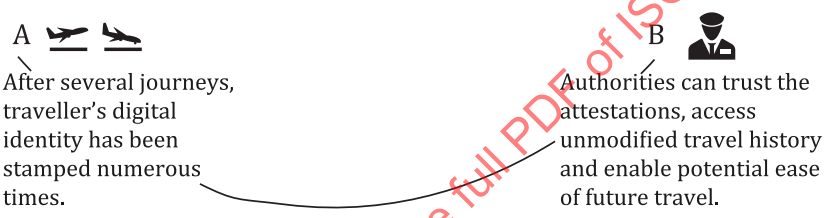


Figure 15 — Improving Known Traveller Digital Identity profile credibility

KTDI™ is a digital identity that includes biometric, biographic and travel history data that enables the traveller to authorize entities in the traveller journey to access selected information about them to allow for risk-rating, verification and access.

Beneficial aspects include:

— Enabling traveller to be a partner in the security process.

— Respecting sovereignty of countries.

— Incorporating the ability to undertake verification and risk assessment.

— Enabling extensive, upfront structured information sharing with entities.

— Risks identified through enhanced opportunity for data exploitation and analysis against other databases.

Potential issues include:

— Requiring trust between entities.

— Privacy risks need to be addressed.

— Government support is critical for success.

The KTDI™ initiative has produced a prototype (see Figure 16 for a blueprint of it), which makes use of four core technologies: distributed ledger, cryptography, biometrics and mobile interface.

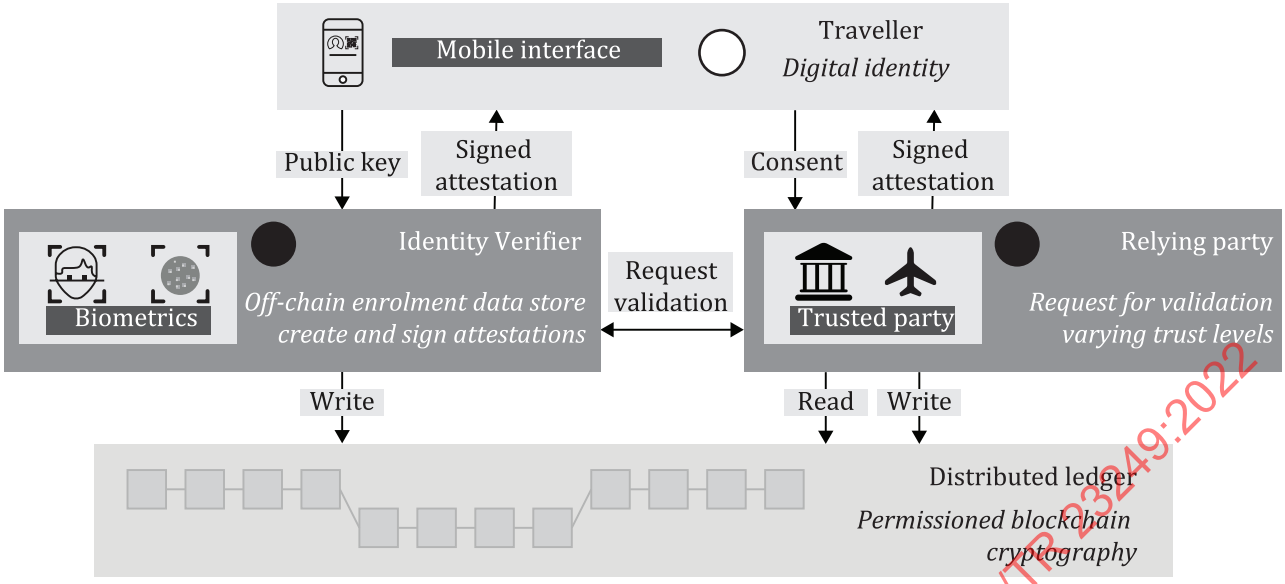


Figure 16 — KTDI™ high-level prototype blueprint

The mobile interface is the traveller's private key store and holds all attestations. The traveller's identity is first verified by their citizenship government (acting as the identity verifier)[13].

Following verification, the traveller's digital identity is created in an enrolment backend, a proof of identity is added to the distributed ledger and an attestation is added to the traveller's digital identity.

Subsequently, the traveller can give consent to a relying party to view and validate their attestations. To do so, the relying party can check the distributed ledger using the traveller's shared public key and subsequently request identity information from the identity verifier. The relying party can then add attestations to the traveller's identity.

The prototype demonstrates important technology barriers to stakeholders and invites experimentation to seek solutions and improve the concept from a technology perspective. Additionally, re-evaluation assesses the prototype feasibility to expand to the wider public and private sector ecosystem.

These processes are based in the Hyperledger Indy, Aries and Ursa initiatives.

6.8 WeIdentity

WeIdentity[5)] is a blockchain-based program for identity management (https://fintech.webank.com/en/weidentity/https://fintech.webank.com/en/weid/). It is built upon a permissioned blockchain platform called FISCO BCOS.

FISCO BCOS architecture features an AMOP (Advanced Messages On-chain Protocol) as a safe and efficient message channel, smart contracts written in Solidity, and an ARPI (Account – Role – Permission – Interface) permission model. FISCO BCOS provides group signatures and ring signatures, that are tamper-resistant, repudiation-resistant, supporting anonymity and traceability.

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

In FISCO BCOS, one-to-one anonymous transfer can be verified by the blockchain nodes without knowing receiver's and sender's identities and amount. In the meantime, a regulator can decrypt the anonymous transfer, by using a tailored ZKP algorithm.

WeIdentity offers a safe and efficient solution for identity authentication and data cooperation based on blockchain. Following W3C DID specifications, WeIdentity is a universal solution for decentralized identity management and trackable data sharing to address problems such as siloed data and data misuse. It is based on the open source solution developed by WeBank and built on top of an open consortium chain.

WeID provides a solid solution for DID and digital credential. WeIdentity Credential offers a complete set of W3C Verifiable Credentials based solutions designated to standardize and digitize such credentials into a verifiable and interchangeable format. The solution also supports Selectively Disclosure of Credential attributes and generating evidence of Credentials on blockchain.

WeIdentity is a solution for decentralized identity management and standardized data exchange, which allows digital identity registration, authentication and management, as well as cross-institutional data sharing in a trusted and compliant manner.

The verification of a credential requires three steps:

1) Registration of a universal ID for a person or entity on the blockchain.

2) Creation of a credential.

3) Endorsement of a verification.

Actors in the system are:

— User: The User is the owner of the self-sovereign identity, who has full control of the identifiers, credentials, authorization and verification.

— Issuer: The Issuer is an organization with the authority to issue or authenticate credentials or other identifier information stored on the blockchain.

— User Agent: The User Agent generates a WeID for the User on blockchain following KYC procedures. The User can access the identifier data via the User Agent as being an authoritative and trustworthy body.

— Verifier: The Verifier is a permitted third party to verify if the credential was issued by an authority issuer and if the credential data was modified.

In summary, WeIdentity DID Module has come with a distributed identification protocol based on FISCO-BCOS Blockchain Platform, and W3C DID specification, to create identities on chain and associate it with any person or object in the real world. Moreover, DID ensures the Entity with full rights of control and ownership of the identities.

6.9 Masterchain

6.9.1 General

Masterchain[6] (https://www.fintechru.org/directions/raspredelennyy-reestr/) is a P2P-network with access control. The communications between the nodes of this network are based on the modified Ethereum protocol. Masterchain provides for safe record of information in a distributed ledger. The copies of this ledger are kept at each node of the network.

6) Masterchain 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.

Identity management is a functional part of the Masterchain application platform. The platform is developed by FinTech Association, a consortium of the largest Russian financial institutions and industrial corporations. The platform development and operation are supervised by the Bank of Russia.

Masterchain is used for mortgage accounting, for banking products in trade finance and as a digital asset marketplace. Identification of system users and business parties or government institutions they represent is done via an accredited certification provider (CP) according to electronic signature laws. Network operator registers entities and their staff by recording credentials into system smart contracts on the blockchain.

Every business process running on Masterchain is represented by a smart contract that has a list of parties engaged and a list of confidential document records. Users and application services request access to documents of interest from the Confidential Messaging Service (CMS) of the platform. CMS issues ephemeral tokens to be signed by the requestor for authentication.

Authorization of requests for confidential files is done by a system smart contract of role model. The contract contains records on what combination of business-party role, user function and data object type can lead to read or write access grant. If authorization succeeds, CMS route the request to other nodes or contact secure storage service containing the requested documents.

The final goal of the project is the creation of a distributed ledger of digital bank guarantees issued by the banks operating in the Russian Federation, as well as moving away from guarantees on paper. It is expected that a digital guarantee will act as a primary digital document, which will be reproduced on paper only if necessary, for the purpose of reference.

The key system principles of Masterchain are as follows:

a. The distributed ledger of Masterchain does not store data requiring special storage mode (commercially sensitive data, personal data, classified data, etc.).

b. The data processed by Masterchain has legal value (in the Russian legal framework).

c. There is no technical need in trusted intermediaries.

d. The network supports the programmable contracts (smart contracts).

e. The system does not have a single point of failure.

f. The resources invested by the members to support the operation of the system are accounted for independently.

g. The system is scalable (according to the number of members and transactions).

Goals of the system are as follows:

a. Elimination of the risk of lacking information necessary to prevent fraudulent transactions.

b. Exchange of information about physical persons (data structure "KYC Attributes") between the members of the Masterchain decentralized network, not involving the disclosure of information covered by bank secrecy or clients' personal data.

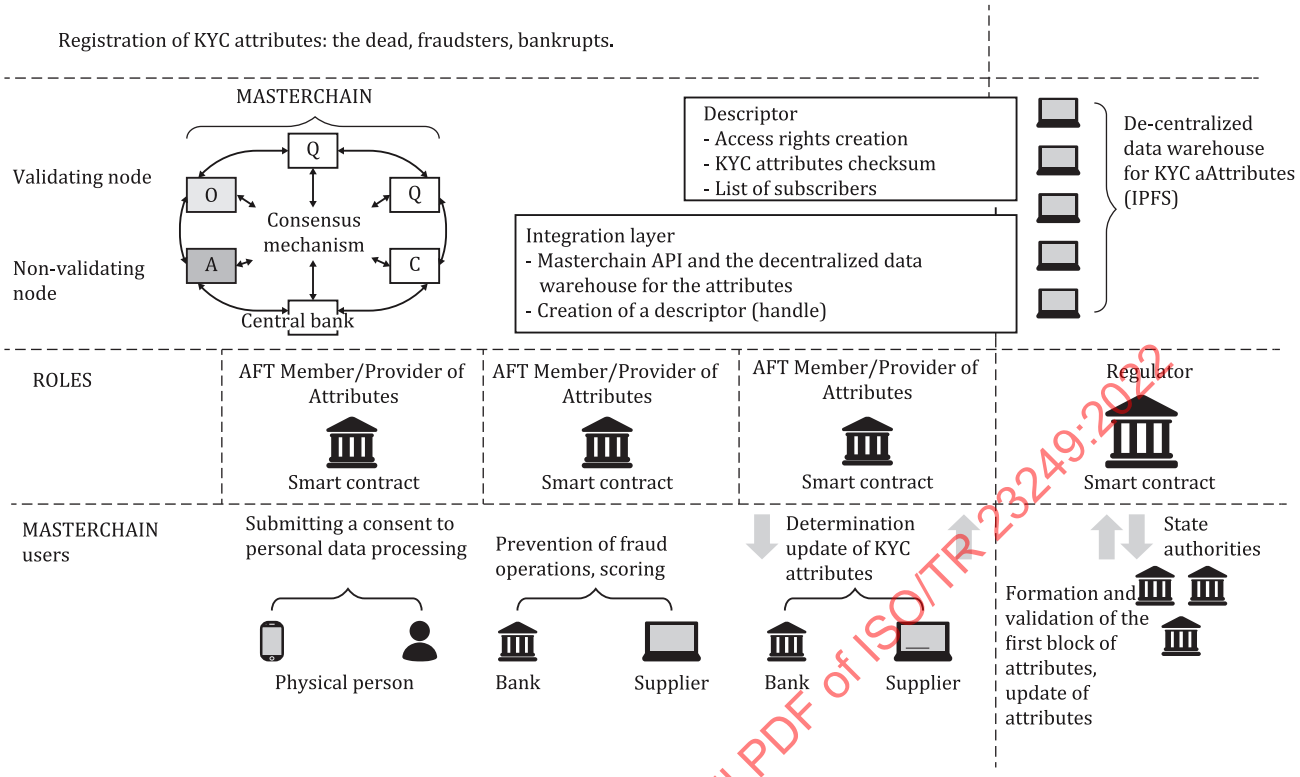
c. Providing the ability to scale the solution in the following areas:

    1. simplified identification - the implementation of the Digital Identity concept;

    2. exchange of information about legal entities;

    3. exchange of credit histories.

The registration of the KYC attributes is as shown in Figure 17.



NOTE Reproduced with permission from fintechru.org

Figure 17 — Registration of KYC Attributes

The database "KYC Attributes" is stored in anonymized form in a decentralized storage (IPFS) integrated with the Masterchain decentralized network, but not in the network itself.

6.9.2 Actors in the system

— Provider: a member of the decentralized network responsible for collection, processing and transfer of the "KYC Attributes" database.

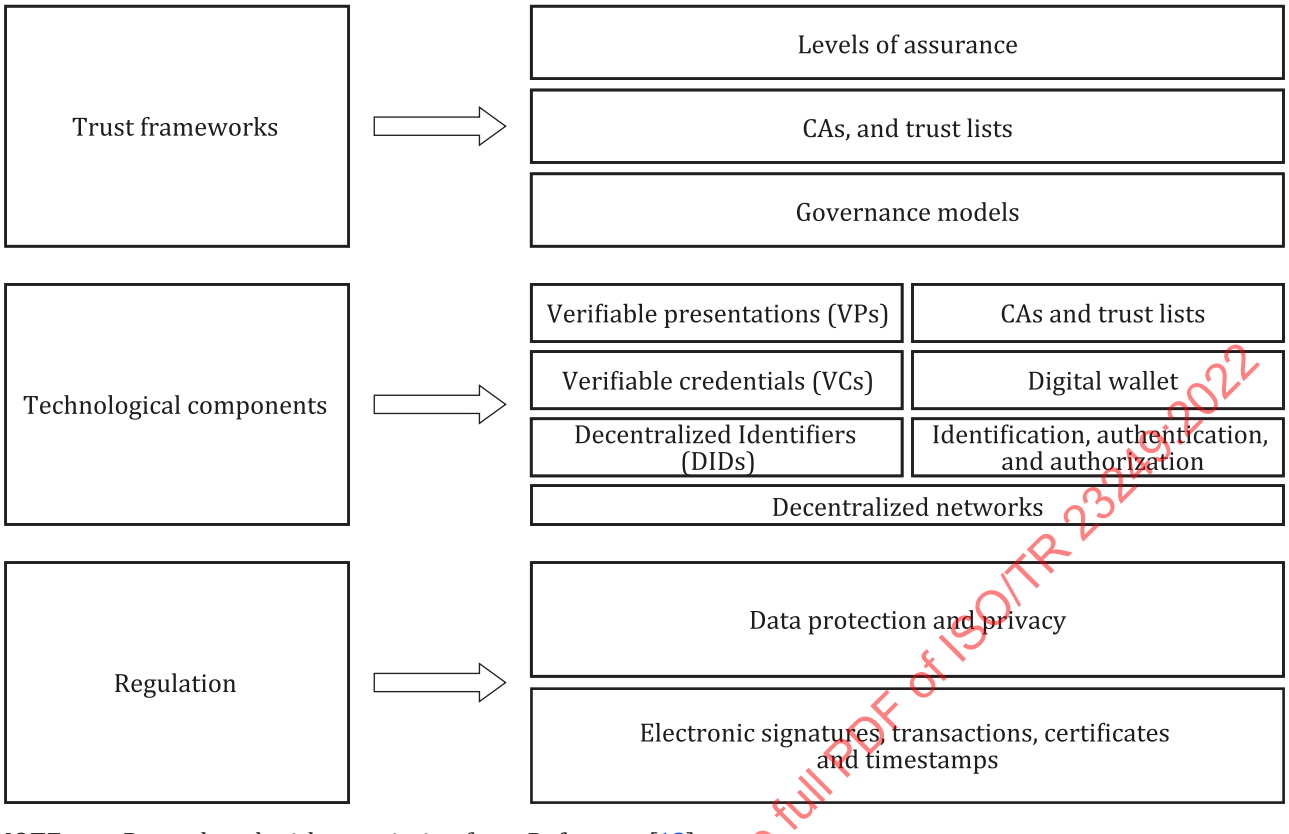
— Consumer: a member of the decentralized network with an access to the "KYC Attributes" database using its data to prevent fraudulent operations.

— Physical person - a person who grants or revokes consent to the processing and use of their personal data for the "KYC Attributes" database.

— Regulator - a person performing control / audit of the selected scenario / process for integrity, compliance with the legislation, and proper execution of inquiries of physical persons.

6.10 LACChain

LACChain ID (https://www.lacchain.net/home) is the second layer of the blockchain-based infrastructure that the LACChain Alliance is making available for enterprise use of blockchain in Latin America and the Caribbean. This second layer complements the first layer of public-permissioned blockchain networks by enabling the authentication and identification of the entities (individuals, organizations, things and processes) using the infrastructure. Assigning proper identifiers allows, as a principal use, to establish the ownership of the digital assets and settle legal accountabilities and responsibilities. The identity layer of LACChain is also essential for the third layer: Tokenized Fiat Money. It would not be possible to tokenize and transfer digital money in compliance with regulations without an identity layer allowing KYC and AML processes.



NOTE Reproduced with permission from Reference [13].

Figure 18 — LACChain ID Stack

LACChain ID model (see Figure 18) is based on seven categories of technological components: Decentralized identifiers (DIDs); verifiable credentials (VCs); verifiable presentations (VPs); authentication, authorization, and identification; digital wallets; certificate authorities (CAs) and trust lists (TLs); and decentralized ledgers (DLTs).

LACChain promotes DID methods that

— are scalable,

— guarantee privacy and pseudonymity,

— register the DIDs in a smart contract with a well-defined governance,

— do not allow to use the same public key as a DID and as an authentication method (if applicable),

— destroy the seed of the DID so it cannot be re-generated by a hacker in case of theft,

— do not disclose any personal data or information in the DID documents,

— store the DID documents in the blockchain, so they can be easily found by issuers or verifiers that require to resolve a specific DID,

— use quantum-safe cryptography for the authentication methods, and

— allow responsible use of biometrics (by the wallets and applications use to operate these DIDs).

LACChain is committed to maintain a DID registry and resolver (similarly to the one managed by DIF, available at https://uniresolver.io) of those DID methods deployed on the LACChain Blockchain Networks that meet the LACChain ID requirements.

LACChain actively promotes verifiable credentials that satisfy the following conditions:

— The DID of the subject and the issuer can be found and resolved from the blockchain.

— Claims data or metadata from the credential are never registered in the blockchain.

— Expiration conditions can be automatically checked from the credential.

— Credential status can be verified against a smart contract living in the blockchain, and nobody but the issuer is able to change it. This eliminates the need of external and/or centralized CRL or OCSP.

— Suspension and revocation of credentials is supported.

The content of a credential includes:

— URI to uniquely identify the credential and/or the subject of the credential (e.g. DIDs).

— URI to identify the issuer (e.g. a DID).

— URI to identify the credential type.

— URI to identify terminology and protocols that allow parties to read the credential.

— Cryptographic proof of the issuer.

— Claims data or metadata to access it.

— Issuance date.

— Expiration conditions.

— Location of the credential status (e.g. a smart contract in a blockchain network).

There are at least three types of exchange of credentials:

— Issuance: The credential is sent from an issuer to the requester, holder, or subject.

— Delegation/Transference: The credential is exchanged between requester, holder and subject.

— Presentation: The credential is sent from a holder to a verifier.

For all the types of exchanges of credentials, the channels between the repository where the credential is stored (i.e. the digital wallet) and the service that generates or consumes the credential is secure and protected.

The preferred format for verifiable credentials and presentations is JSON-LD.

LACChain ID introduces the LACChain ID Verification Process, consisting in the following steps: verification of the digital wallet; verification of the validity of the credential (or validation); verification of the status of the credential; verification of the issuer; verification of the presenter; and verification of the claims.

The LACChain ID framework relies on decentralized ledgers to store the cryptographic proofs of the DIDs, the cryptographic proofs and status of the verifiable credentials and presentations, the public keys of the certificate authorities, and the trust lists, among others.

6.11 Decentralised digital architecture based on blind signatures

6.11.1 General

Reference [3] provided a conceptual architecture for a decentralized digital identity system that satisfies constraints evaluated as essential for the protection of human rights, elaborating eight requirements