TECHNICAL REPORT

ISO/TR 23644

First edition
2023-05

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

Reference number
ISO/TR 23644:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies*, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

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

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

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

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

1 Scope

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Abbreviated terms

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

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

5 Types of trust anchors

5.1 Overview

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.2 Legal trust anchors

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

Examples of relevant legislation include:

— national policy and infrastructure;

— national security;

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

— property regulation, real estate, intellectual property;

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

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

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

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

5.3 Data trust anchors

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

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

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

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

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

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

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

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

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

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

— health patient records and prescription drug purchases;

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

— databases of utility companies for proof of address;

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

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

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

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

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

5.4 Cryptographic trust anchors

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

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

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

5.5 Cybersecurity trust anchors

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

— Identify: The identification of risks.

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

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

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

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

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

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

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

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

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

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

— the node architecture, implementation and operation;

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

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

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

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

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

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

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

— establishment of trust anchors for the mechanisms to use.

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

5.6 Social trust anchors

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

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

The majority of decentralized identity management models rely on a specific (often centralized) certification or verification service to provide a level of assurance (LoA). This LoA is representational to the level of trust the RP can have regarding the relationship between the "real-life" identity [e.g. natural person, legal person, internet of things (IoT) device] and the identifier used to represent them within the identity management system.

In many instances, a centralized trust service is provided by a known, recognized and authoritative entity (e.g. government department, regulated service provider, licensed entity). However, there are examples of novel approaches and architectures. These architectures view trust as being determined by the communication of a series of verifiable relational links between network participants.

The network-based trust models have also been termed "web of trust", "socially verified" or "graph-based" models of trust. The proposed architectures imply that the root of trust lays within the network, specifically the component relationships and explicit relations that can be verified by chains of cryptographically verified interaction between participants. Ultimately, the assurance is distributed across a number of network participants allowing for a LoA to be communicated to those inside and outside of the network (i.e. the RP).

These trust models are based on architectures proposed to be more similar to real life, where assurance of an identity (and its identifier) is distributed across a number of other identities (and their identifiers). A common example provided in the literature is when a potential employer telephones a number of "references" to check the presented attributes and characteristics asserted by the potential employee. In this example, trust is distributed through the social web of the candidate, which is similar (in this instance) to distributing trust through a network of participants in the context of decentralized digital identity management systems.

6 Existing trust anchors for DLT-based identity management

6.1 Overview

There are many different types of trust model and they use these trust anchors differently. The greater the risks (particularly regulatory), the higher the LoA and the need for strong authentication in a way that is assured or certified by government. Hence, government authoritative sources usually operate at LoA 3 or 4, and also provide a root trust anchor in a chain of trust where the downstream credential issuers can be commercial operators supporting industry or consumer purposes.

Until recently, most digital credentials were authenticated between the user and the authority, and the authority issued an assertion or authentication result to the RP. However, recently there has been increased interest in the concept of self-sovereign identity (SSI), where the user holds a credential issued by the authoritative source and controls its use in a consent model; this can be done using a stateless or a stateful trusted intermediary, where the credential is held in the intermediary or held by the user in a secure device, e.g. trusted execution environment (TEE) in a mobile phone. Depending on the policy, the RP can choose whether or not to accept the credential held by the user, or to verify the credential against the issuing authority. While the verification can normally succeed, the verification can fail for reasons of elapsed time or policy exceptions, which can be anticipated in the risk mitigation strategy.

There are other models and technologies that rely on various mixes of authentication factors, which can also affect the architecture.

EXAMPLE A two-sided model at the end point. An authenticator exists in the user device. The user and the device authenticate to the authenticator on one side (locally) and the network interacts (externally) with the other side of the authenticator. Europay, MasterCard® and Visa® (EMV) Worldpay[1)] operate this way.

1) MasterCard® and Visa® are examples of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of these products.

Some of these models are listed below:

— cryptographic trust anchors in PKI;

— federated PKI;

— social trust anchor architectures;

— autonomic identifiers used as cryptographic trust anchors;

— data trust anchors in eID regulations – eIDAS regulation;

— data trust anchors in non-PKI-based SSI solutions using DIDs;

— data trust anchors in non-PKI-based, non-DID partial SSI solutions using zero knowledge proof (ZKP).

6.2 Cryptographic trust anchors in public key infrastructures

ITU-T Recommendation X.509 | ISO/IEC 9594-8 defines a set of frameworks for public key certificates and attribute certificates upon which full services can be based. IETF has extensive experience in the treatment of cryptographic trust anchors, especially in PKI. Some DLT-based identity management systems are based in PKI.

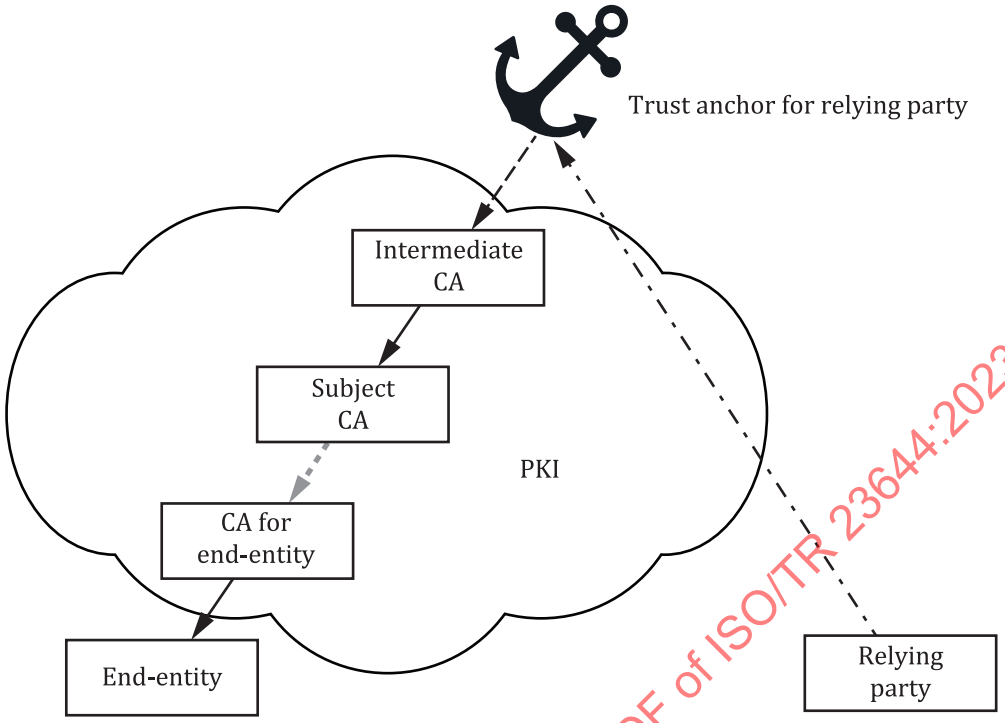
IETF RFC 5280, the X.509 profile technical specification for the internet, refers to trust anchors in the context of the validation of certification paths, as part of the certification validation procedure, but it does not define what a trust anchor is.

According to IETF RFC 5914:2010, "a trust anchor is an authoritative entity represented by a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information or actions for which the trust anchor is authoritative".

Moreover, according to IETF RFC 5934:2010, "a trust anchor contains a public key that is used to validate digital signatures". This specification differentiates three types of trust anchors: apex trust anchors, management trust anchors and identity trust anchors. The latter "are used to validate certification paths, and they represent the trust anchor for a public key infrastructure", being "most often used in the validation of certificates associated with non-management applications".

IETF RFC 6024:2010 states that "a trust anchor represents an authoritative entity via a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information for which the trust anchor is authoritative. An RP uses trust anchors to determine if a digitally signed object is valid by verifying a digital signature using the trust anchor's public key, and by enforcing the constraints expressed in the associated data for the trust anchor".

In the IETF model, trust anchors are used as "roots" of hierarchical PKIs, thus supporting chains of trust, i.e. an end-entity digital signature is verified with the end-entity's public key included in a certificate signed by a subordinate certification authority (CA); the subordinate CA's signature is verified with the subordinate CA's public key included in a certificate issued by a root CA; this root public key is a typical example of a trust anchor, as seen in Figure 1:



Key

certifies
chain of CAs
trust anchor certifies CA
trust relationship

NOTE Source: ISO/IEC 9594-8:2020, Figure 2.

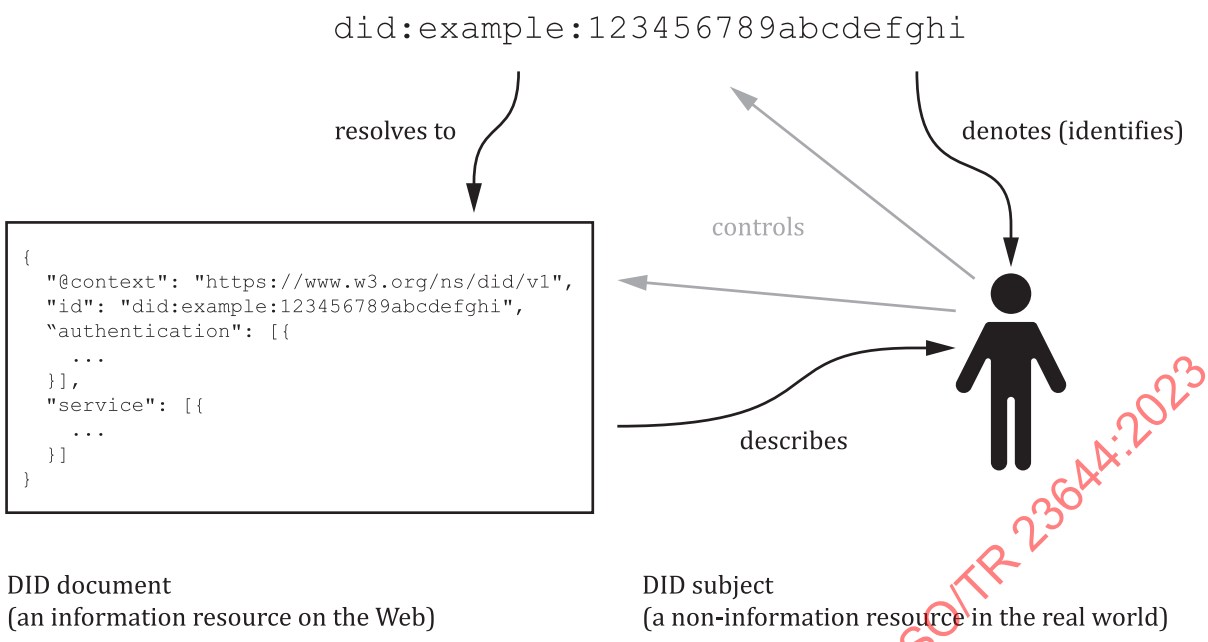
Figure 1 — Example chain of trust

Trust anchor collections can be, and usually are, represented by a trust anchor list, conforming to the syntax defined in IETF RFC 5914, with the aim to publish them to applications (trust anchor stores) used by RPs when validating a digital signature. This trust anchor list is typically signed to protect and authenticate the information contained within.

The concept of trust anchor, initially defined in the context of hierarchical PKIs, later was adopted for decentralized PKI and used, e.g. in SSI management systems.

From a technical perspective, this verifiable, self-sovereign digital identifier is based on a type of identifier called a "decentralized identifier" (DID), and, in technical terms, it is a URL, i.e. an identifier universal or uniform resource locator, with its own rules of syntax and processing, that relates a subject with a DID document, and which describes how such DID is used, and, in particular, how the DID document supports the authentication of the subject associated with the DID, as shown in Figure 2.

One of the peculiarities of a DID is that it is based in DLT or other forms of decentralized networks, so it does not require a centralized registration system. This allows the implementation of a decentralized public key infrastructure (DPKI), a combination of DIDs for decentralized identification and a decentralized key management system (DKMS). This is in opposition to the classic hierarchical PKI systems, which are precisely based on the centralization of the issuing function in the hands of a provider, although with nuances. In fact, the PKI is not an absolutely centralized system either, but there are multiple providers, with their own PKIs, that compete with each other, which has forced trust models to be established that are somewhat decentralized (although it can be said that the centralization of trust management has shifted towards trusted lists and browsers).



NOTE Source: Reference [44].

Figure 2 — Relationships between DID, DID document and subject

Thus, DKMS is proposed as a new approach to cryptographic key management intended for use with blockchain and DLTs where there are no centralized authorities, inverting the core assumption of conventional PKI architecture, namely that public key certificates will be issued by centralized or federated CAs, because with DKMS the initial "root of trust" for all participants is any distributed ledger that supports a DID.[44]

Starting from a DID (e.g. did:example:123456789abcdefghi), anyone can go to the internet to obtain the corresponding DID document that describes the DID in question (an operation called "DID resolution"), and use its contents to authenticate the subject and to obtain attributes or claims about it, such as name and surname, or other personal information to share. The DID document can be stored on chain or off chain, if compliance with data protection regulations is needed. Consideration is given as to whether a DID is being stored on-chain for a natural person, especially with regards to data protection compliance. Another identified use of the cryptographic trust anchor relates to the prior setup required by certain protocols for anonymous credentials, such as the Camenisch-Lysyanskaya signature scheme[28] or the cryptographic accumulator system used for non-revocation proof currently implemented by Hyperledger®[2] Indy-Aries-Ursa technologies.[39]

6.3 Cryptographic trust anchors — Federated PKI

PKI Federation has already been outlined. Figure 3 shows just the top-level CAs in the US Federal Government Federal PKI Bridge[49] and its external federation through the Federal Bridge Certification Authority (FBCA) to a wide range of external CAs. Some of these, such as the CertiPath bridges, extend out to major CAs supporting global corporations (such as Boeing, Northrop Grumman and Lockheed Martin) and industries, as well as linking to other governments, such as the Netherlands Ministry of Defence. Hundreds more CAs exist under the US Federal Common Policy which are not shown in Figure 3.

2) Hyperledger® 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.

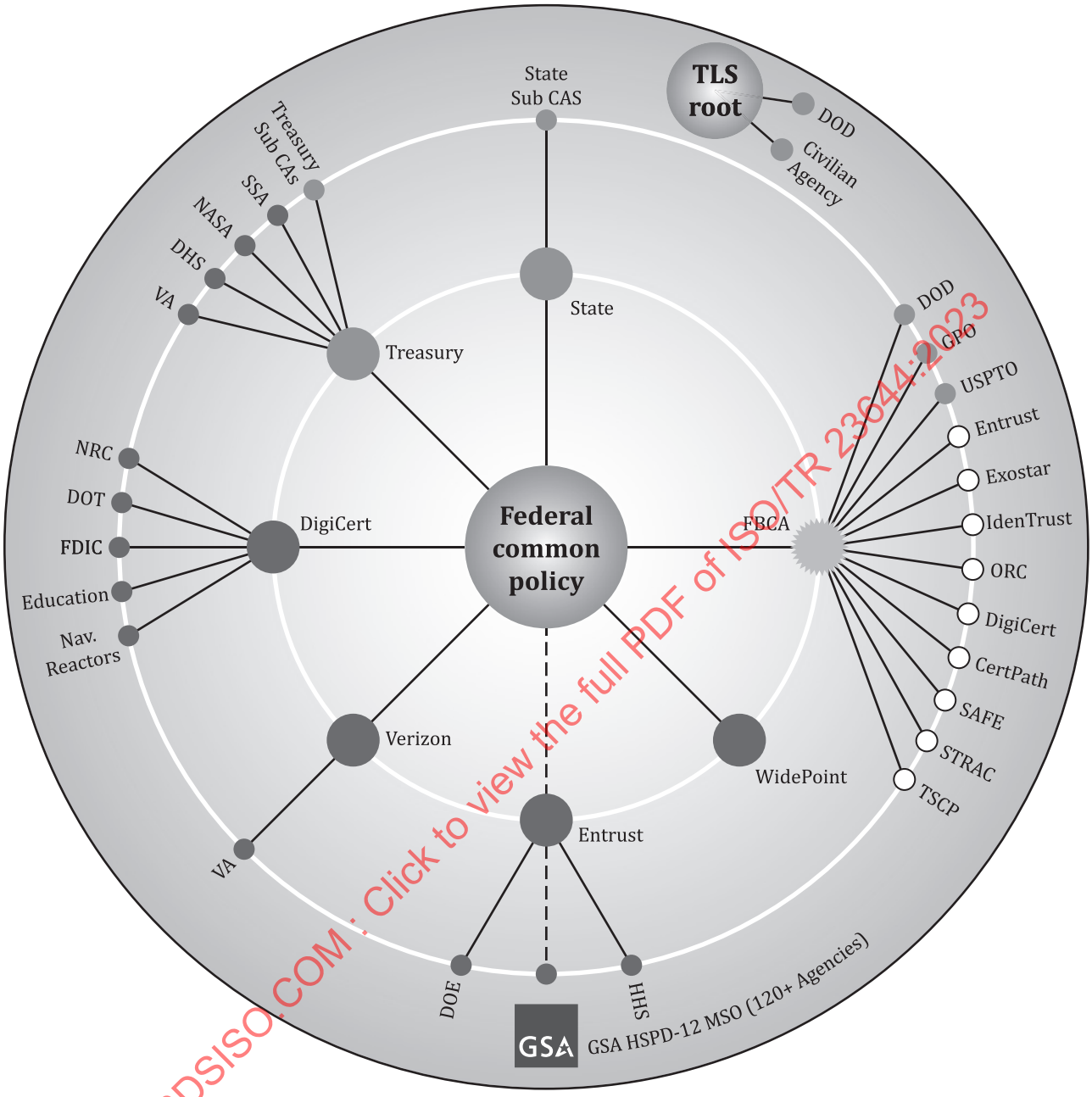


Figure 3 — US PKI Federation

Many other governments operate similarly large PKI federations within and across government organizations and with industry, particularly in Asia. The opportunity for cross-border inter-federation is significant and this is expected to grow as IoT, payments, logistics sensors, mobile and autonomous sensors and smart cities increase.

There are several key features about PKI federation, including:

— the certificate contains information for the RP to be able to navigate to the issuing certificate authority, where the certificate can be validated; this is known as path discovery and validation;

— there can be resilience between multiple CAs using cross-signing;

— the user is required to authenticate to the issuing CA, so the CA can send an attestation or validation response back to the RP;

— certificates contain references to policy object IDs, which are stored offline; a certificate typically supports one policy OID for a specific set of policies at an appropriate LoA for a given use case scenario;

— certificates usually exist within a hardware token/smartcard or device, which can hold multiple certificates to support authentication [logical access control system (LACS)], digital signature, encryption, secure email and physical access control system (PACS) to buildings, etc.;

— it is crucial to maintain the security of all CAs, especially when using hierarchical CA structures, e.g. if a root CA is affected by a security issue, all following CAs in the chain of trust are affected as well.

The business use cases for PKI federation are almost exclusively for government and industry employees involved in highly regulated and collaborative activities at LoA 3 and 4.

A few national citizen eID schemes are based on PKI standards and so they can, theoretically, federate with other nations. However, at present, there are no known citizen or consumer PKI federations. This is a possibility in the future, particularly once the challenges of cross-technology federation are addressed, including identity-related resources description, registration, access control, service level agreements, usage policies, management, life cycle, operational procedures, legal framework and provider/user incentives, among others.[52]

Many of the lessons learnt in the establishment and governance of PKI federations can be applicable to the decentralized identity management systems that need to connect and interoperate. Thus, it is possible to imagine federations of different decentralized identity management systems which are based in diverse DLT networks and systems, by using specific technologies such as Polkadot sharded protocol[51], that enable cross-blockchain transfers of any type of data or asset.

6.4 Social trust anchor architectures

Examples of social trust anchor architectures are found within the BrightID whitepaper[25] and also the "pre-formal digital identity" proposal outlined by Immorlica et al.[37]

Immorlica et al.[37] propose that the following two "graph-based relationship-flow" metrics are required to be considered in order to measure trust:

— The maximum flow which provides the maximum length of the route that is to be verified by the RP in order to provide a LoA concerning the overall graph-based relationship flow.

— The probability of the claim which provides a risk calculation representing the trust in the claim according to pre-agreed determinants. These determinants can include how many of the identifiers in the flow are known and verified previously by the RP, or how many of the identifiers are verified and recognized by entities such as government authorities, licensed authorities, etc.

In a similar vein, BrightID provides a number of analysis methods for achieving a "uniqueness score" to enable a specific LoA. They include, but are not limited to:

— metadata, to combine actual relationship or "trustflows" to other data points available to the RP;

— thresholds, which is an algorithmic-based risk calculation of whether any identity is a Sybil (fake identity) or not.

There are computational, algorithmic and privacy concerns with both of these frameworks, especially if they are proposed to be used in isolation for achieving a high degree of assurance within decentralized identity management systems.

There exists another subjective approach, based on reputation measures gathered and shared by a distributed community. The reputation-based trust can be considered as a viable, complementary solution for achieving trust in DLT-based identity management system.

Users assign ratings to service or resource providers. Those ratings represent a judgement of their direct interactions' quality. Eventually, trust is computed from the aggregation of ratings concerning local experiences, taking into account the feedback that is being provided by other network entities.

6.5 Cryptographic trust anchors — Autonomic identifiers

Key event receipt infrastructure (KERI) is a proposal for an identity system based secure overlay for the internet, authored by Samuel M. Smith,[45] supporting an "autonomic identity system", formed by autonomic identifiers, that have self-managing or self-governing capabilities, and autonomic namespaces, that have a self-certifying prefixes which provides cryptographic verification of root control authority over their namespaces.

The autonomic identity system has an associated decentralized key management infrastructure (DKMI), where the primary root-of-trust are self-certifying identifiers that are strongly bound at issuance to a cryptographic signing (public, private) key-pair, which are self-contained until/unless control needs to be transferred to a new key-pair. In that event, an append only chained key-event log of signed transfer statements provides end verifiable control provenance, meaning that the log can be verified by any end user that receives a copy.

No trust in intervening infrastructure is needed to verify the log and validate the chain of transfers and thereby establish the current control authority. Because any copy of the record or log of transfer statements is sufficient, any infrastructure providing a copy is replaceable by any other infrastructure that provides a copy, enabling the use of ambient infrastructure to provide a copy of the log. The combination of end verifiable logs served by ambient infrastructure enables ambient verifiability, allowing anyone to verify anywhere at any time.

The primary key management operation is key rotation (transference) via a key pre-rotation scheme. Two primary trust modalities are considered: a direct (one-to-one) mode and an indirect (one-to-any) mode. In the direct mode, the identity controller establishes control via verified signatures of the controlling key-pair. The indirect mode extends that trust basis with witnessed key event receipt logs (KERL) as a secondary root-of-trust for validating events.

The security and accountability guarantee of indirect mode are provided by KERI's agreement algorithm for control establishment among a set of witnesses, but it can employ a distributed consensus ledger when considered appropriate.

Because KERI is event streamed, it enables DKMI that operates in-stride with data events streaming applications where performance and scalability are more important. Also, the core KERI engine is identifier independent, supporting a universal portable DKMI.

This can be the case when using KERI combined with a DLT-anchored DID method to support portability or interoperability.

6.6 Data trust anchors in eID regulations – eIDAS Regulation

Cryptographic trust anchors defined by the internet PKI community have evolved into different types of trust anchor, especially with the emergence of trust services. In addition to being used to establish and validate a cryptographic chain of trust, they are now recognized to be legal trust anchors because there is legislation that regulates the trustworthiness of credentials issued by providers, which are supervised under that legislation.

As an illustrative example, in the European Union and the European Economic Area, the main legal instrument regulating trust in electronic transactions is Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (from now on, eIDAS Regulation).

Article 1 of the eIDAS Regulation:

— lays down the conditions under which Member States recognize electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;

— lays down rules for trust services, in particular for electronic transactions;

— establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

Trust anchors are regulated in Article 22 of the eIDAS Regulation. More specifically, according to paragraph (1) of this Article, each Member State is mandated to establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

Alongside to these national trust lists, under paragraph (4) of Article 22, the Commission is obliged to make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing, in an instrument known as a list of trusted lists.

The legal rules for the management of these lists is being developed further as a result of the Commission Implementing Decision (EU) 2015/1505 of 8 September 2015, which lays down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market (text with European Economic Area relevance). This implementing decision adopts ETSI TS 119 612 v2.1.1 as a syntax for the representation of trust anchors, using an extensible markup language (XML) schema definition (XSD) vocabulary that considers PKI-based and non-PKI-based trust services.

The main objective of the trust list is to provide confidence to RPs about the trustworthiness of qualified trust service providers and, as such, it can be described as a "trust representation mechanism"[35] associated to a legal trust anchor.

This mechanism can be useful in the context of decentralized and distributed identity systems willing to rely on existing trust services. It is interesting from an international perspective also because the United Nations Commission on International Trade Law (UNCITRAL) is proposing legislation for the international recognition of eIDs and trust services, an instrument that can help shape transnational legal trust anchors.

The eIDAS Bridge project[34], led by the European Commission in the context of the European Blockchain Services Infrastructure (EBSI) initiative, has analysed the possibility of inheriting trust in decentralized identity (a DID) by leveraging the usage of PKI certificates (e.g. under eIDAS regulation). This can be supported in different ways, but three prominent possibilities are as follows:

a) Certifying the public key associated with the private key used to control the DID, especially if the DID is cryptographically derived from that public key. This is a classic chain of trust because the DID is verifiable against a trust anchor, both from the cryptographic and legal perspective.

b) Associating the DID (controlled with a user-generated key pair) with a pre-existent X.509v3 certificate. This case is described as a trust bridge between two digital signature systems.

c) Associating a verifiable credential (VC) (referred to a DID) with a pre-existent X.509v3 certificate. This is described as a trust bridge between the VC attributes and the certificate attributes.

In all these scenarios, the X.509v3 certificate uses the corresponding hierarchical trust anchor, but the certificate can also be considered as a data trust anchor itself (assuming a legal trust anchor exists

regulating this possibility), in respect to one or more identity attributes of the DID owner (assuming a legal trust anchor exists ruling this scenario, i.e. in terms of liability).

NOTE In eIDAS, these identity attributes include the minimum data required for the confirmation of the identity of the certificate subject regulated in Annex I and Annex III..

This approach is shown in Figure 4.

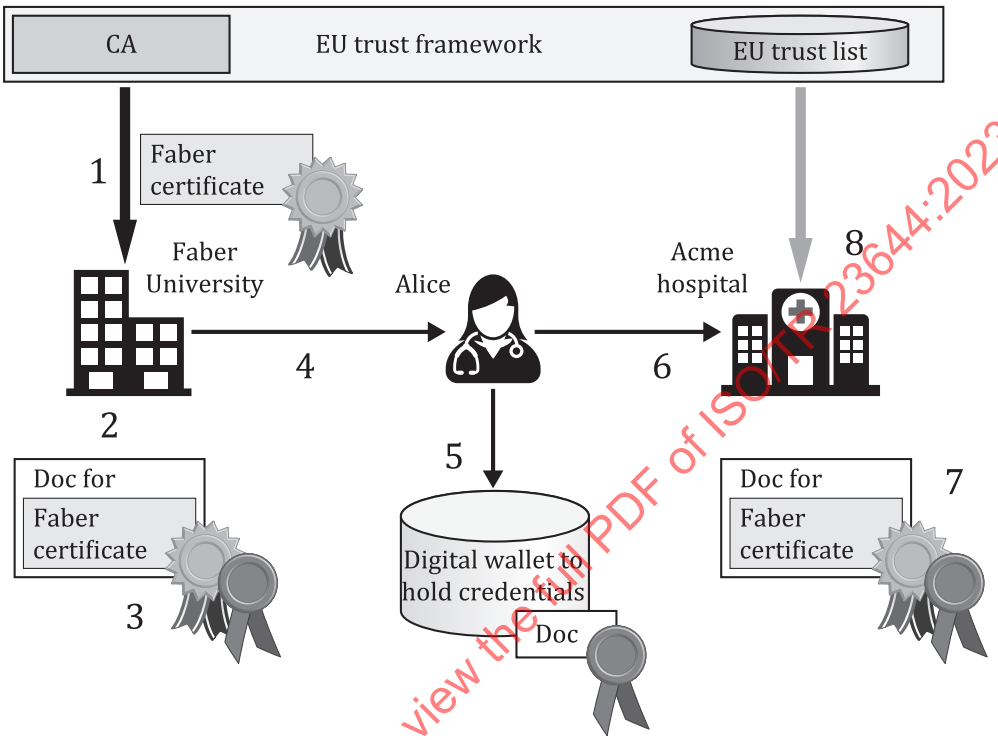


Figure 4 — Verifiable claims

Another possible way to inherit trust in the identification data contained in a DID or, more probably, a VC, is to link the DID with the identity attributes provided by a notified eID scheme. As stated in a report from the EU Commission[32]:

> "in this case, the link of the DID with the eIDAS minimum data set can be done by allowing the user agent managing the DID to perform an eIDAS authentication, acting as a service provider. This authentication could be done at the moment of the creation of the DID, or later. In order to ensure the trustworthiness of the link, the user agent needs to guarantee that the legitimate owner of the DID is the same person that is authenticating via eIDAS. After creating the link, the identification data coming from the eIDAS Minimum Data Set would become part of the attributes that the user could disclose to third parties".

NOTE Electronic identification means are not trust services in the eIDAS Regulation.

An eIDAS identification can be considered a data trust anchor for one or more identity attributes of the DID owner, but not a cryptographic trust anchor nor necessarily a data trust anchor in all cases. Thus, in the same report from the EU Commission[32], it is said that:

> "from the point of view of those third parties, these identification data would be self-asserted, as they cannot rely on the eIDAS node to verify them [...] because eIDAS eID is meant to be used for authenticating when accessing to services, but not for providing claims about identity that can be verified by others different from those who are requesting the authentication".

If this interpretation is considered correct, there is a need to modify the eIDAS regulation so it can be considered an appropriate legal trust framework, or to create a new contractually based legal trust anchor that reuses and extends eIDAS Regulation in its current and/or a future form.

6.7 Data trust anchors in non-PKI-based SSI solutions using DIDs

In Sovrin's provisional trust framework, a "trust anchor" was defined as "An Issuer who is considered by a Verifier or a Governance Authority to be authoritative for a particular set of Claims or Credentials. A Trust Anchor may be: a) informally recognized as a Trust Anchor by one or more Verifiers, b) formally designated as a Trust Anchor by a Governance Authority, or c) Accredited as a Trust Anchor by an Accreditation authority", while a "trust anchor credential" was "A Credential issued by a Governance Authority or an Auditor asserting that an Issuer is Accredited to serve as a Trust Anchor".[46]

Figure 5 depicts the layers of the Sovrin Infrastructure.[46] As shown, the trust anchor appears in layer 4, governance frameworks, due to its consideration as a legal trust anchor in contractual agreements.

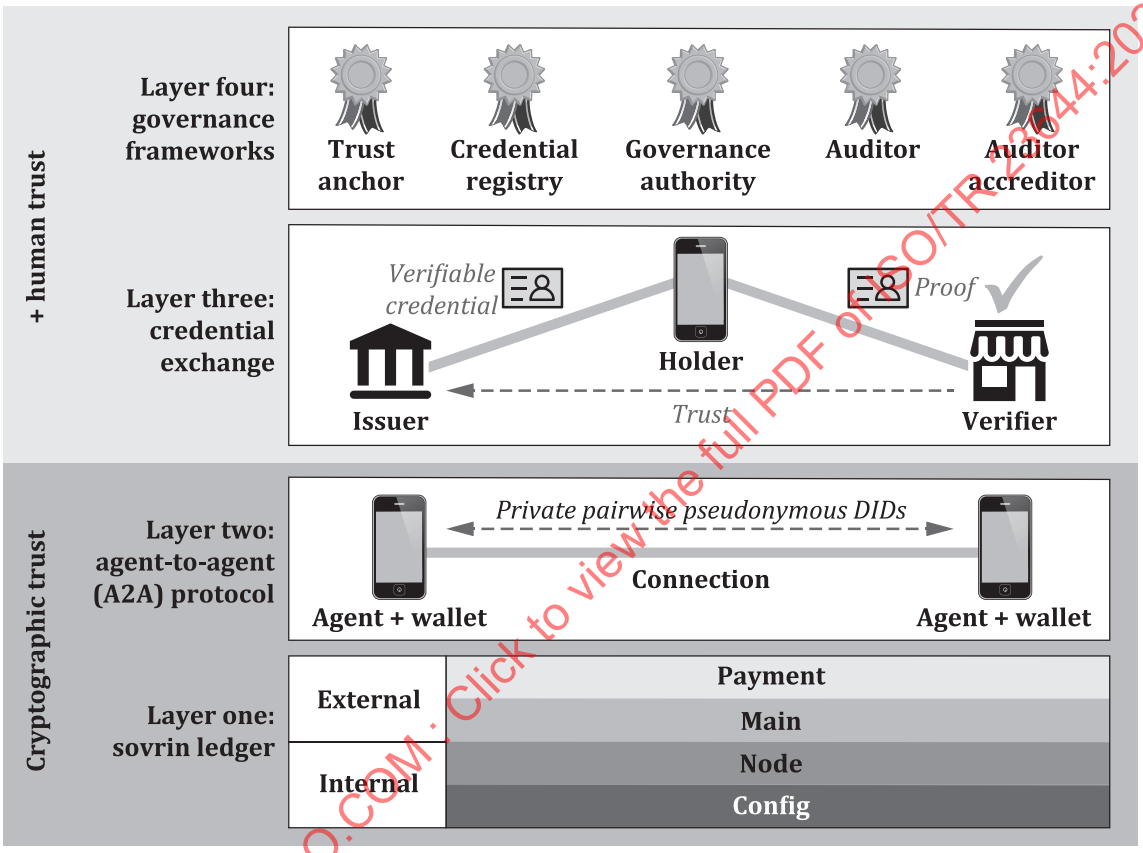


Figure 5 — Sovrin infrastructure

In the Sovrin Governance Framework V2, the term "trust anchor" has been deprecated and substituted by the term "transaction endorser", defined as "an Organization authorized under Permissioned Write Access to authorize a Transaction by digitally signing it so it will be accepted by a Validator Node. The Transaction Endorser role is only needed for Permissioned Write Access. It is not needed for Public Write Access".[46] This change does not seem to affect the role that trust anchors have in the Sovrin system, as the transaction endorser is only one example of a trust anchor.

One business use case example of a trust anchor role is a "university diploma: in many cases, a Verifier will only accept Proof of a diploma if the Issuer of the Credential is the university itself".[46] However, the binding of the claimed diploma credential to the user with foundational identity information (normally from the public authorities' trust anchors) is missing from the university model. How does the university prove that the person did properly learn and qualify for the diploma and that they were who they claimed to be throughout the education process? How does the national authority prove that the university is accredited and competent for the course and qualifications provided? Both questions highlight existing problems with fraud and impersonation in many countries.

It is also important to note the concept of a "trust anchor credential", which is "A Credential issued by a Governance Authority or an Auditor asserting that an Issuer is Accredited to serve as a Trust Anchor",[46] which follows a chain of trust model.

Figure 6[46] shows a conceptual diagram of the roles in the Sovrin Governance Framework layer, including the trust anchor role:

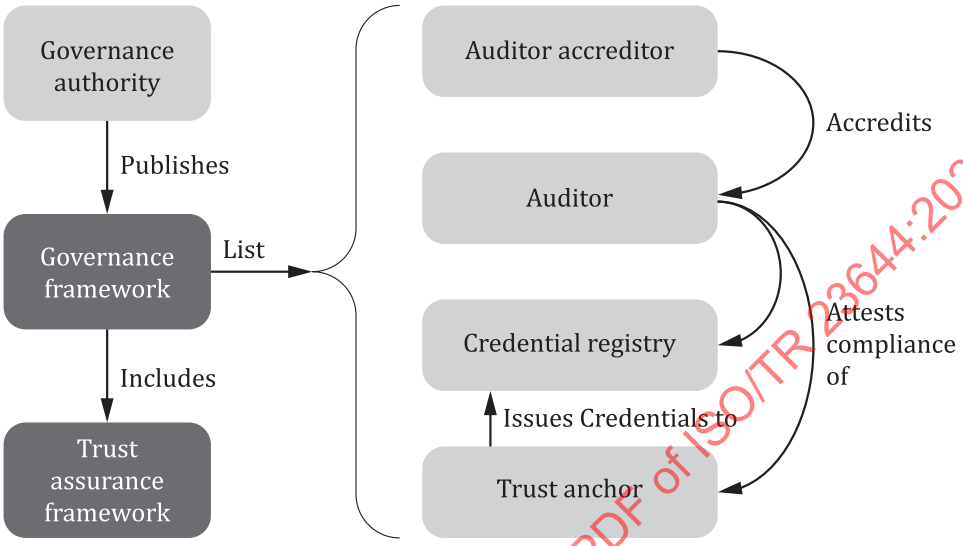


Figure 6 — Sovrin governance framework

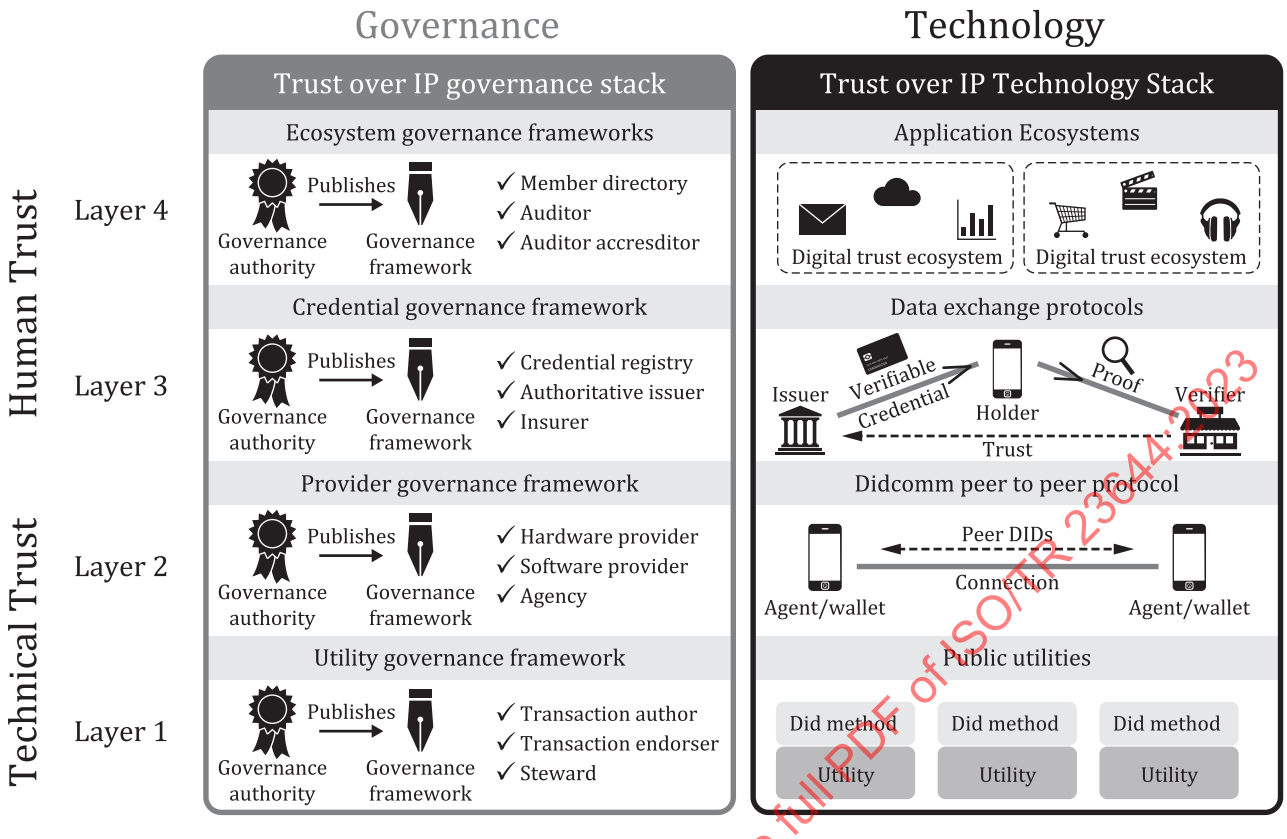
The Sovrin system allows for the implementation of different policies regarding trust anchors, including informal trust anchor management, usage of credential registries (that serve a similar purpose as trust anchor stores) or formal designation after accreditation.

Hyperledger Aries™[2] is one of the Hyperledger projects hosted by The Linux Foundation. It provides a shared, reusable and interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credentials. It 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.

As Hyperledger Aries was initially developed with input from developers from Sovrin Foundation, among others. Hyperledger Aries' recent RFC trust over IP (ToIP) stack[29] tends to follow the Sovrin model, introducing a complete architecture for internet-scale digital trust that integrates cryptographic trust in the machine layer with human trust in the business, social and legal layers.

In this model, "Layer One and Layer Two together enable the establishment of cryptographic trust (also called technical trust) between peers. By contrast, the purpose of Layers Three and Four is to establish human trust between peers—trust between real-world individuals and organizations and the things with which they interact (devices, sensors, appliances, vehicles, buildings, cities, etc.)",[29] and it mandates support for different proof types, including ZKP.

As shown in Figure 7, a trust anchor is considered in layer 3 as an authoritative issuer of a credential under a governance framework, configuring it as a data trust anchor, a special type of credential issuer that is able to assure the identity attributes.



NOTE Source: Reference [29].

Figure 7 — Trust layers in ToIP

From the perspective of verifiers, there is often the need to verify that a credential was issued by an authoritative issuer, i.e. trust anchor. The ToIP stack gives governance authorities several mechanisms for designating trust anchors, including:

a) DID documents, meaning that for a relatively small set of trust anchors, the governance authority can publish the list of trust anchor DIDs in a DID document on one or more DID networks of its choice;

b) VCs, meaning the governance authority (or its designated auditors) can issue VCs to the issuers which they in turn can provide directly to verifiers or indirectly via credential holders;

c) credential registries, meaning that for search and discovery, a governance authority can also publish VCs for each trust anchor to a credential registry.

This approach (to be extended, purportedly, by the recently announced Trust Over IP Foundation[48]) can be usable in other contexts, where the public sector acts as an authority approving these trust anchors. Some examples proposed are the British Columbia's Verifiable Organizations[26] or the Verifiable Organizations Network[27].

In the EU, this approach can be based in the Internal Market Information System[33], operated by the European Commission.

6.8 Data trust anchors in non-PKI-based, non-DID partial SSI solutions using ZKP

ZKP is the ability of two or more parties to prove they hold the same information but without exposing or sharing that information in any way. ZKP has significant use to preserve privacy, to achieve business decisions without data compromise, to address cross-border challenges and to address challenges

of conflicting policy and legislation. ZKP technologies come in many forms; the most advanced have developed additional capabilities. The ZKP model:

— completely avoids the exchange of personal data;

— can operate in a federation and inter-federation model using ZKP verification engines (ZVEs);

— can support both SSI and non-SSI models simultaneously to meet complex policy requirements that can change;

— avoids the stateful trusted intermediary such as DID and DID document;

— avoids some operational, security, legal and privacy vulnerabilities, including man-in-the-middle and replay attacks;

— enables authoritative sources to notify changes directly to an RP without user participation, particularly to support legal requirements;

— supports fine grain consent management, backed by a full audit trail;

— supports multi-party computation (MPC) for situations where several parties working together cannot expose sensitive information (e.g. for cross-border AML) yet all parties will know the outcome of the computation, but there is no way they can know how it is done using the distributed computational model;

— will soon have artificial intelligence (AI) tools to assist users in the protection of their personal data and to manage complex consent;

— supports power of attorney, delegations and proxies, particularly to support care workers for the elderly and vulnerable, and parents of children and young adults;

— can increasingly support federation or inter-federation between technology types;

— can provide a privacy preserving, one-time link between on chain integrity and off chain personal data;

— can include high assurance KYC and AML;

— can support cross-border complex multi-jurisdictional situations;

— can support bound high-assurance payments and crypto-currency transactions;

— is dependent on access to high assurance authoritative data sources as trust anchors.

7 Using trust anchors

7.1 Representing multiple dimensions of risk

Each of these trust anchors presents a different dimension to understanding and measuring the risk parameters. Each dimension can vary independently from the others and is therefore a vector. To measure all the dimensions results in a matrix of values or vectors.

In reality, the values in each vector are interrelated because the risks and their mitigations are related, so the vectors are interrelated. This is reflected in the history of cybersecurity and trust measurement, as follows:

— The original Orange Book (US Department of Defence Trusted Computer System Evaluation Criteria) contained a matrix of four divisions of measures for confidentiality, availability and integrity, under headings for accountability (identification, authentication, auditing), assurance, policy and documentation.