Approved Version

2019-12-04

Sovrin Glossary V3

This document is part of the Sovrin Governance Framework V2. This is the Living Community Version—please visit this link to the official approved version. If you have comments or suggestions, we invite you to contribute them to this document—access is open to anyone. If you are interested in joining the Sovrin Governance Framework Working Group, please visit our Meeting Page.

Purpose

The purpose of the Sovrin Glossary is (a) to help readers of the Sovrin Governance Framework (SGF) and its Controlled Documents to understand the meaning of the terms that the authors intended to convey, and (b) to help authors of the SGF—and Domain-Specific Governance Frameworks based on it—to convey such meaning in a consistent fashion. Because the SGF addresses the full spectrum of business, legal, and technical policies for Self-Sovereign Identity, the audience for this Glossary includes business analysts, product managers, lawyers, policymakers, regulators, CIOs, compliance officers, software architects, software developers, and IT professionals. The Glossary includes the level of detail needed to accurately document and administer the Sovrin Governance Framework.

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

A

A2A

Acronym for Agent-to-Agent. See Agent-to-Agent Protocol.

Accreditation

The service an Auditor performs of verifying that a Trust Community Member conforms to the requirements of a Governance Framework. Accreditation involves performing an assessment against relied upon criteria for the benefit of adding reasonable assurance that the assessed party is meeting those criteria.

Accreditation Credential

A Credential issued by an Auditor Accreditor or Governance Authority asserting that a Trust Community Member conforms to the Accreditation requirements of a Governance Framework. See Appendix H.

Accredited

The status of an Entity having a valid Accreditation Credential from an Auditor for a specific Governance Framework.

Active Thing

A Man-Made Thing that has the capacity to operate its own Agent(s) that can interact using the Agent-to-Agent Protocol. Examples include computing devices, drones, robots, vehicles, satellites, active cat collars, etc. Active Things still require Thing Controllers. Mutually exclusive with Passive Thing. See Appendix B and Appendix C.

Agency

A service provider that hosts Cloud Agents and may provision Edge Agents on behalf of Entities. Agencies may be Unaccredited, Self-Certified, or Accredited. See Appendix F.

Agent

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. See Appendix F.

Agent-to-Agent (A2A) Protocol

A protocol for communicating between Agents to form Connections, exchange Credentials, and have other secure private Interactions. The Sovrin Protocol is a specific Agent-to-Agent Protocol. A less technical synonym is DID Communication. See Appendix F.

Agent-to-Agent Protocol Layer

The Sovrin Infrastructure Layer for peer-to-peer Connections and Interactions over the Agent-to-Agent Protocol. See Appendix F.

Agent-to-Agent Protocol Layer Roles

The business roles defined at the Agent-to-Agent Protocol layer of Sovrin infrastructure. These include Agency and Developer. See Appendix F.

Anonym

A DID used exactly once, so it cannot be contextualized or correlated beyond that single usage. See also Pseudonym and Verinym.

Anywise

A non-reciprocal relationship rooted in the Identity of one party, where the other party is the public (a faceless “other” that can be instantiated without bound). For an Organization to issue publicly Verifiable Credentials, its Issuer DID must be on a public ledger such as the Sovrin Ledger. It is thus an Anywise DID—a DID to which any other Entity may refer without coordination. The term “public DID” is sometimes used as a casual synonym for “Anywise DID”. However, “public DID” is deprecated because it is ambiguous, i.e., it may refer to a DID that is world-visible but usable only in pairwise mode, or to a DID that is not published in a central location but nonetheless used in many contexts, or to a DID that is both publicly visible and used in Anywise mode. Compare N-wise and Pairwise.

Assurance

See Trust Assurance.

Attribute

An Identity trait, property, or quality of an Entity. A small set of Attributes of a Sovrin Entity, including its Public Key(s) and Service Endpoint(s), may be recorded on the Sovrin Ledger (specifically the Sovrin Domain Ledger). A private Attribute of a Sovrin Entity may be asserted by a Claim in a Credential.

Auditor

An Individual or Organization that performs Accreditation on behalf of a Governance Authority. See Appendix H.

Auditor Accreditor

An Organization authorized by a Governance Authority to issue Auditor Credentials under a particular Governance Framework. Auditor Accreditation involves assessing the competence and qualifications of Auditors accepted within the relevant jurisdiction against generally accepted audit standards. See Appendix H.

Auditor Accreditor Credential

A Credential issued by a Governance Authority asserting that an Auditor Accreditor is authorized to issue Auditor Credentials for a particular Governance Framework. See Appendix H.

Auditor Credential

A Credential issued by a Governance Authority or an Auditor Accreditor asserting that an Auditor is authorized to perform Accreditation for a particular Governance Framework. See Appendix H.

B

C

Claim

An assertion about an Attribute of a Subject. Examples of a Claim include date of birth, height, government ID number, or postal address—all of which are possible Attributes of an Individual. A Credential is comprised of a set of Claims. *(Note: In the first version of the Sovrin Trust Framework, this term was used the same way it was used in the early W3C Verifiable Claims Working Group specifications—as a synonym for what is now a Credential. That usage is now deprecated.)*

Cloud Agent

An Agent that is hosted in the cloud. It typically operates on a computing device over which the Identity Owner does not have direct physical control or access. Mutually exclusive with Edge Agent. A Cloud Agent requires a Wallet and typically has a Service Endpoint. Cloud agents may be hosted by an Agency. See Appendix F.

Cloud-to-Cloud Connection

A Connection between Cloud Agents. See Appendix F.

Connection

A cryptographically verifiable communications channel established using an Agent-to-Agent Protocol between two DIDs representing two Entities and their associated Agents. Connections may be Edge-to-Edge Connections or Cloud-to-Cloud Connections. Connections may be used to exchange Verifiable Credentials or for any other communications purpose. Connections may be encrypted and decrypted using the Public Keys and Private Keys for each DID. A Connection may be temporary or it may last as long as the two Entities desire to keep it. Two Entities may have multiple Connections between them, however each Connection must be between a unique pair of DIDs. A relationship between more than two Entities may be modeled either as Pairwise connections between all of the Entities (Peering) or each Entity can form a Connection with an Entity representing a Group. See Appendix A and Appendix F.

Connection Invitation

An Agent-to-Agent Protocol message type sent from one Entity to a second Entity to invite the second

Entity to send a Connection Request. See Appendix A and Appendix F.

Connection Request

An Agent-to-Agent Protocol message type sent from one Entity to a second Entity to request to form a Connection. See Appendix A and Appendix F.

Controlled Document

A subdocument of a Governance Framework that is included by reference in the Master Document as a normative component of the framework. A Controlled Document is typically able to be revised independently from the Master Document, permitting a modular legal architecture. For the Sovrin Governance Framework, a list of Controlled Documents is included as Appendix A to the Sovrin Governance Framework Master Document. The present document (the Sovrin Glossary) is a Controlled Document.

Controller

An Identity Owner that is responsible for control of another Entity—specifically the Private Keys needed to take actions on behalf of that Entity. For example, a Thing Controller has a Controller relationship with a Thing. It is one of three types of identity control relationships described in Appendix C.

Core Principles

The principles published in a Governance Framework that apply broadly to all Trust Community Members. The Core Principles of the Sovrin Governance Framework are defined in Section 2 of the Sovrin Governance Framework Master Document.

Credential

A digital assertion containing a set of Claims made by an Entity about itself or another Entity. Credentials are a subset of Identity Data. A Credential is based on a Credential Definition. The Entity described by the Claims is called the Subject of the Credential. The Entity creating the Credential is called the Issuer. The Entity holding the issued Credential is called the Holder. If the Credential supports Zero Knowledge Proofs, the Holder is also called the Prover. The Entity to whom a Credential is presented is generally called the Relying Party, and specifically called the Verifier if the Credential is a Verifiable Credential. Once issued, a Credential is typically stored by an Agent. (In Sovrin Infrastructure, Credentials are not stored on the Sovrin Ledger.) Examples of Credentials include college transcripts, driver licenses, health insurance cards, and building permits. See also Verifiable Credential. See Appendix A and Appendix G.

Credential Definition (CredDef)

A machine-readable definition of the semantic structure of a Credential based on one or more Schemas. In Sovrin Infrastructure, Credential Definitions are stored on the Sovrin Ledger. Credential Definitions must include an Issuer Public Key. Credential Definitions facilitate interoperability of Credentials and Proofs across multiple Issuers, Holders, and Verifiers.See Appendix G.

Credential Offer

An Agent-to-Agent Protocol message type sent from an Issuer to a Holder to invite the Holder to send a Credential Request to the Issuer. See Appendix G.

Credential Request

An Agent-to-Agent Protocol message type sent from a Holder to an Issuer to request the issuance of a Credential to that Holder. See Appendix G.

Credential Exchange

A set of Interaction Patterns within an Agent-to-Agent Protocol for exchange of Credentials between Entities acting in Credential Exchange Roles. See Appendix G.

Credential Exchange Layer

The Sovrin Infrastructure Layer for Credential Exchange. As the SSI ecosystem matures, additional human trust-building protocols may appear at this layer, such as protocols for staking, reputation sharing, or insurance. See Appendix G.

Credential Exchange Layer Roles

The business roles defined at the Credential Exchange layer of Sovrin Infrastructure. These include Subject, Issuer, Holder/Prover, Verifier, and Insurer. See Appendix G.

Credential Registry

An Entity that serves as a Holder of Credentials issued by Trust Community Members in order to provide a cryptographically verifiable directory service to the Trust Community or to the public. The term also refers to the actual repository of Credentials maintained by this Entity. An informal Credential Registry may accept Credentials from participants whose purpose is to cross-certify each other’s roles in the Trust Community. A formal Credential Registry may be authorized directly by a Governance Authority or Accredited by an authorized Auditor for the relevant Governance Framework. See Appendix H.

Credential Registry Credential

A Credential issued by a Governance Authority asserting that a Credential Registry is authorized under a particular Governance Framework. See Appendix H.

Cryptographic Trust

Trust bestowed in a set of machines (Man-Made Things) that are operating a set of cryptographic algorithms will behave as expected. This form of trust is based in mathematics and computer hardware/software engineering. Compare with Human Trust. See Appendix D.

D

Data Center

The physical facility hosting a Sovrin Network component such as a Node or an Agency.

Data Controller

As defined by the EU General Data Protection Regulation (GDPR), the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

Data Processor

As defined by the EU General Data Protection Regulation (GDPR), a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of a Data Controller.

Data Protection by Design

A widely recognized set of principles for protecting Personal Data. Specific Sovrin Data Protection by Design principles are a subset of the Core Principles in the Sovrin Governance Framework.

Data Subject

As defined by the EU General Data Protection Regulation (GDPR), any person whose Personal Data is being collected, held, or processed. In the Sovrin Governance Framework, a Data Subject is referred to as an Individual.

Decentralization by Design

A set of principles developed by the Sovrin Foundation to build decentralization into systems from the very start. The Decentralization by Design principles are a subset of the Sovrin Core Principles.

Decentralized Identifier (DID)

A globally unique identifier developed specifically for decentralized systems as defined by the W3C DID specification. DIDs enable interoperable decentralized Self-Sovereign Identity management. A DID is associated with exactly one DID Document. The Sovrin Technical Governance Board defines the technical specifications for a Sovrin DID in the Sovrin DID Method Specification.

Delegate

An Identity Owner that acts on behalf of another Identity Owner. Formally, a Delegate is the Holder of a Delegation Credential. See Appendix C.

Delegation

The act of one Identity Owner, the Delegator, authorizing another Identity Owner to act as a Delegate. In the Sovrin Network, Delegation is accomplished by the Delegator issuing a Delegation Credential to the Delegate. Note that Delegation is not Impersonation. Delegation is one of three types of identity control relationships described in Appendix C.

Delegation Credential

A Credential issued by an Identity Owner—the Delegator—to authorize another Identity Owner to act as a Delegate. See Appendix C.

Delegator

An Identity Owner who enters into a Delegation relationship with a Delegate by issuing a Delegation Credential.

Dependent

An Individual whose circumstances or capabilities in a given context requires dependence on a Guardian to administer the Individual's Identity Data. Under the Sovrin Governance Framework, all Dependents have the right (though perhaps not the circumstances or capabilities) to become Independents. Mutually exclusive with Independent. See Appendix C.

Developer

An Individual or Organization that develops hardware or software providing the functionality of any component of Sovrin Infrastructure, including Nodes, Wallets, and Agents. See Appendix F.

DID

Acronym for Decentralized Identifier.

DID Communication

Synonym for Agent-to-Agent Protocol.

DID Document

The machine-readable document to which a DID points as defined by the W3C DID specification. A DID document describes the Public Keys, Service Endpoints, and other metadata associated with a DID. A

DID Document is associated with exactly one DID.

DID Method

A specification that defines a particular type of DID conforming to the W3C DID specification. A DID Method specifies both the format of the particular type of DID as well as the set of operations for creating, reading, updating, and deleting (revoking) it. See Sovrin DID Method Specification.

DID Resolver

A software module that takes a DID as input and returns a DID document by invoking the DID Method used by that particular DID. Analogous to the function of a DNS resolver.

DID Subject

The Entity identified by a DID.

DKMS

Decentralized Key Management System, an emerging standard for interoperable cryptographic key management based on DIDs. In Sovrin Infrastructure, the DKMS standard applies to Wallets and Agents.

DKMS Protocol

A subset of the Agent-to-Agent Protocol that enables Agents to perform DKMS functions for interoperable digital Wallet management, e.g., key exchange, automated backup, offline recovery, social recovery, etc. See Appendix F.

Domain-Specific Governance Framework

A Governance Framework designed to achieve the trust objectives of a specific Trust Community that inherits and/or aligns its Core Principles, Core Policies, and other definitions from a more general Governance Framework. The Sovrin Governance Framework is designed to serve as a general model for Domain-Specific Governance Frameworks based on the Sovrin Web of Trust Model. See Appendix H.

E

Edge Agent

An Agent that operates at the edge of the network on a local device, such as a smartphone, tablet, laptop, automotive computer, etc. The device owner usually has local access to the device and can exert control over its use and authorization. Mutually exclusive with Cloud Agent. An Edge Agent may be an app used directly by an Identity Owner, or it may be an operating system module or background process called by other apps. Edge Agents typically do not have a publicly exposed Service Endpoint in a DID Document, but do have access to a Wallet. Note that the local device may itself be an Active Thing with its own Agent, and for which the Identity Owner is the Thing Controller. See Appendix C and Appendix F.

Edge-to-Edge Connection

A Connection that forms and/or communicates directly between two Edge Agents. See Appendix F.

Endorser

See Transaction Endorser.

Entity

As used in IETF RFC 3986, Uniform Resource Identifier (URI), a resource of any kind that can be uniquely and independently identified. An Entity identified by a Sovrin DID is a Sovrin Entity. See also Identity.

F

Fee Table

See Sovrin Ledger Fee Table.

Founding Steward

A Steward whose service to the Sovrin Network began by executing the *Sovrin Founding Steward Agreement* and hosting a Node under the first version of the Sovrin Governance Framework, formally called the Sovrin Provisional Trust Framework.

G

Genesis Transactions

The first Transactions written to a ledger or blockchain that establish starting conditions upon which all future evolution of ledger state depend. The Genesis Transactions for the Sovrin Main Network ledger were written on 31 July 2017 and defined the initial set of Trustees, Stewards, and Nodes.

Governance Authority (GA)

The Entity (typically an Organization) governing a particular Governance Framework such as a Domain-Specific Governance Framework. Depending on the design of the Governance Framework, the Governance Authority may be responsible for issuing Trust Anchor Credentials, Credential Registry Credentials, Auditor Credentials, or Auditor Accreditor Credentials. A Governance Authority may also issue a Governance Authority Credential to another Governance Authority to cross-link two Governance Frameworks. See the Sovrin Web of Trust Model and Appendix H.

Governance Authority Credential

A Credential issued by one Governance Authority asserting the recognition of another Governance Authority. See Appendix H.

Governance Framework

The set of business, legal, and technical definitions, policies, specifications, and contracts by which the members of a Trust Community agree to be governed in order to achieve their desired Levels of Assurance. Typically divided into a Master Document and a set of Controlled Documents. A Governance Framework is itself governed by a Governance Authority. A Governance Framework is also known as a Trust Framework. The Sovrin Governance Framework is a specific instance of a Governance Framework that is designed to both govern Sovrin Infrastructure and support other Domain-Specific Governance Frameworks. See Appendix H.

Governance Framework Layer

The Sovrin Infrastructure Layer for implementing Governance Frameworks, particularly Domain-Specific Governance Frameworks. See Appendix H.

Governance Framework Layer Roles

The business roles defined at the Governance Framework layer of Sovrin Infrastructure. These include Governance Authority, Trust Anchor, Credential Registry, Auditor, and Auditor Accreditor. See Appendix H.

Group

An Entity that exists to provide a Connection between other Entities. An Organization that is represented by an Entity is an example of a Group. Compare Peering.

Guardian

An Identity Owner who administers Identity Data, Wallets, and/or Agents on behalf of a Dependent. A Guardian is different than a Delegate—in Delegation, the Identity Owner still retains control of one or more Wallets. With Guardianship, an Identity Owner is wholly dependent on the Guardian to manage the Identity Owner’s Wallet. See Appendix C.

Guardianship

The legal responsibility of serving as a Guardian. In Sovrin Infrastructure, Guardianship maps to the rights and responsibilities defined in prevailing legal constructs such as parent, in loco parentis, legal capacity, and power of attorney. Note that Guardianship is not Impersonation or Delegation. While the term Guardianship in this glossary applies strictly to natural persons (Individuals) as Dependents, in a more general sense the term can also be applied to Natural Things (such as pets or animals).

Guardianship is one of three types of identity control relationships described in Appendix C.

Guardianship Credential

A Credential issued to a Guardian by an Identity Owner who has the legal authority to assign a Guardian for a Dependent. See Appendix C.

H

Holder

A role played by an Entity when it is issued a Credential by an Issuer. The Holder may or may not be the Subject of the Credential. (There are many use cases in which the Holder is not the Subject, e.g., a birth certificate where the Subject is a baby and both the mother and father may be Holders. Another case is a Credential Registry.) If the Credential supports Zero Knowledge Proofs, the Holder is also the Prover. Based on the definition provided by the W3C Verifiable Claims Working Group. See Appendix G.

Hosting Provider

A Data Processor that provides hosting services to a Steward or an Agency.

Human Trust

Trust bestowed in a set of humans (Individuals and/or Organizations) that they will behave as expected. This form of trust is based in human social, business, and legal relationships. Compare with Cryptographic Trust. See Appendix D.

Hyperledger

An initiative of the Linux Foundation to develop open source distributed ledger and blockchain technology. The Hyperledger home page is https://wiki.hyperledger.org/. See Hyperledger Indy.

Hyperledger Indy

An open source project under the Hyperledger umbrella for decentralized Self-Sovereign Identity. The source code for Hyperledger Indy was originally contributed to the Linux Foundation by the Sovrin Foundation. Sovrin Stewards run the Hyperledger Indy Node software to operate their Nodes. The Hyperledger Indy home page is https://wiki.hyperledger.org/display/indy.

I

Identifier

A text string or other atomic data structure used to provide a base level of Identity for an Entity in a specific context. In Self-Sovereign Identity systems, Decentralized Identifiers (DIDs) are the standard Identifier. See Appendix A.

Identity

Information that enables a specific Entity to be distinguished from all others in a specific context. Identity may apply to any type of Entity, including Individuals, Organizations, and Things. Note that Legal Identity is only one form of Identity. Many technologies can provide Identity capabilities; the Sovrin Governance Framework defines one such system. See Appendix A.

Identity Data

The set of data associated with an Identity that permits identification of the underlying Entity. In Self-Sovereign Identity, the sharing of Identity Data is under the control of the Identity Owner. See also Sovrin Identity Data. See Appendix A.

Identity Owner

This term refers to the subclassifications of Sovrin Entity that may be held legally accountable. Identity Owners includes Individuals and Organizations but do not include Things. The actual legal accountability of an Identity Owner for any particular action depends on many contextual factors including the laws of the applicable Jurisdiction, Guardianship, and so forth. An Identity Owner may play any of the Sovrin Infrastructure Roles. See Appendix F.

Impersonation

The act of one Entity assuming the Identity of another Entity, often for malicious purposes. Guardianship is not Impersonation because the Guardian is acting on behalf of and with the authorization of the Identity Owner, and is often legally knowable. Delegation is not Impersonation because the Delegate has a recognizable identity distinct from that of the Delegator. See Appendix C.

Inclusive by Design

A widely recognized design practice for building inclusion into systems, products, services, and buildings from the very start. Specific Inclusive by Design principles for Sovrin Infrastructure are a subset of the Core Principles of the Sovrin Governance Framework.

Independent

An Individual who directly controls the Private Key(s) and Link Secret(s) required to administer a set of Sovrin Identity Data and thus is not dependent on any other party for control (other than the Developer of the software and/or hardware for an Agent or Wallet used by that Individual). For any particular set of Sovrin Identity Data, this definition is mutually exclusive with Dependent. Note that it is possible for the same Identity Owner to be both an Independent for some Sovrin Identities and a Dependent for others. See Appendix C.

Individual

A natural person. Mutually exclusive with Organization.

Industry Sector

An area of distinct economic activity as defined by the World Trade Organization. See https://www.wto.org/english/tratop_e/serv_e/mtn_gns_w_120_e.doc.

Insurer

A service provider who provides insurance to Issuers for the potential liability of asserting a Credential or to Verifiers or Relying Parties for the potential risk of relying on a Credential. See Appendix G.

Interaction

A set of messages exchanged over a Connection using an Agent-to-Agent Protocol. See Appendix F.

Interaction Pattern

An orchestrated set of Interactions that defines a subprotocol of an Agent-to-Agent Protocol. Credential Exchange is one type of Interaction Pattern. See Appendix F.

Issuer

The Entity that issues a Credential to a Holder. Based on the definition provided by the W3C Verifiable Claims Working Group. See Appendix G.

Issuer Public Key

The special type of cryptographic key required for an Issuer to issue a Credential that supports Zero Knowledge Proofs. In Sovrin Infrastructure, the Issuer Public Key is published in the Credential Definition.

J

Jurisdiction

A legally defined scope of authority to which an Identity Owner is bound by law at any one point in time. Jurisdiction is particularly relevant to Sovrin Governance Framework policies in order to help ensure diversity among Stewards. For these purposes, Jurisdiction is defined broadly as: sovereign states or autonomous regions that are members of the United Nations, any UN Specialized Agency, or the Universal Postal Union, as well as sovereign states or autonomous regions that have observer status at the UN or any UN Specialized Agency.

K

Key Recovery

The process of recovering access to and control of a set of Private Keys—or an entire Wallet—after loss or compromise. Key Recovery is a major focus of the emerging DKMS standard for cryptographic key management. See also Recovery Key.

L

Ledger-Wide Tombstone

A Tombstone marked across the entire Sovrin Ledger so that it is no longer returned by any Node in response to requests for read access. Mutually exclusive with Node-Specific Tombstone.

Legal Identity

A set of Attributes sufficient to identify an Identity Owner for the purpose of legal accountability in at least one Jurisdiction. A Legal Identity may be established by one or more valid Credentials from Issuers that are trusted to provide the necessary Attributes.

Level of Assurance (LOA)

A measure—usually numeric—of the Trust Assurance that one Entity has in another Entity based on a defined set of criteria that establish the amount of reliance the first Entity may accept from the second Entity in the performance of the criteria. LOAs are often defined in or referenced by Governance Frameworks.

Link Secret

An item of Private Data used by a Prover to link a Credential uniquely to the Prover. A Link Secret is an input to Zero Knowledge Proofs that enables Claims from one or more Credentials to be combined in order to prove that the Credentials have a common Holder (the Prover). A Link Secret should be known only to the Prover.

M

Man-Made Thing

A Thing generated by human activity of some kind. Examples include manufactured goods, houses, cars, books, documents, and digital files. Man-Made Things include both Active Things and Passive Things. Mutually exclusive with Natural Thing. See Appendix B and Appendix C.

Master Document

The controlling document of a Governance Framework. The Master Document typically references a set of Controlled Documents constituting the rest of the framework. See Sovrin Governance Framework Master Document.

Microledger

A cryptographic data structure maintained over a single Connection that enables two or more Agents to securely share Pairwise DIDs, Public Keys, Service Endpoints, and other Identity Data. See Sovrin Microledger.

N

Natural Thing

A Thing that exists in the natural world independently of humans. Examples include animals, pets, plants, mountains, rivers, etc. Natural Things by definition do not have the capacity to operate their own Agent(s) and thus must always have a Thing Controller. Mutually exclusive with Man-Made Thing (which must also have a Thing Controller too). See Appendix B and Appendix C.

Node

A computer network server running an instance of the code necessary to operate a distributed ledger or blockchain. In Sovrin Infrastructure, a Node is operated by a Steward running an instance of the Sovrin Open Source Code to maintain the Sovrin Ledger. A Node must be either a Validator Node or an Observer Node. See Appendix E.

Node Selection Algorithm

An algorithm specified by the Sovrin Technical Governance Board in the *Sovrin Steward Technical*

Policies document (see Appendix A of the Sovrin Governance Framework Master Document) that automatically selects the current active set of Validator Nodes at any one point in time.

Node-Specific Tombstone

A Tombstone marked by an individual Steward so that it is no longer returned in response to a request for read access to the Node operated by that Steward. Mutually exclusive with Ledger-Wide Tombstone.

N-wise

A direct relationship between a limited number of entities, N, such that N is greater than 2, and such that the Identity of each party is understood in the same way by all participants. A doctor-patient-hospital relationship is N-wise, as is a nuclear family relationship among siblings. Compare with Pairwise and Anywise. See also Peering.

O

Open Governance

A governance model in which the Governance Authority is open to public participation, operates with full transparency, and does not favor any particular contributor or constituency. The Sovrin Foundation operates under an Open Governance model.

Open Source License

Any form of intellectual property license approved and published by the Open Source Initiative.

Open Standards

Technical standards that are developed under an Open Governance process; are publicly available for anyone to use; and which do not lock in users of the standard to a specific vendor or implementation. Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption. Many Open Standards have implementations that are available under an Open Source License.

Observer Node

A Node that maintains a read-only copy of the Sovrin Ledger. A Node may be able to operate as either an Observer Node or Validator Node, but at any one point in time it must operate in only one of these two roles. There is no restriction on who may run an Observer node or how many they may run because the responses from Observer Nodes may be verified using State Proofs.

Organization

A legal Entity that is not a natural person (i.e., not an Individual). Examples of Organizations include a

Group, sole proprietorship, partnership, corporation, LLC, association, NGO, cooperative, government, etc. Mutually exclusive with Individual.

Other Entity

An Entity identified on a network external to the Sovrin Network.

Overlay

A data structure that provides an extra layer of contextual and/or conditional information to a Schema. This extra context can be used by an Agent to transform how information is displayed to a viewer or to guide the Agent in how to apply a custom process to Schema data. In Sovrin Infrastructure, Overlays are stored on and accessed from the Sovrin Ledger and can therefore be both searched for and provided by reference to an Agent.

P

Pairwise

A direct relationship between exactly two Entities. Most relationships in the Sovrin ecosystem are Pairwise, even when one or both Entities are not Individuals. For example, business-to-business relationships are pairwise by default. A DID or a Public Key or a Service Endpoint is Pairwise if it is used exclusively in a Pairwise relationship. Compare with N-wise and Anywise.

Passive Thing

A Man-Made Thing that does not have the capacity to operate its own Agent(s). Examples include documents, books, non-computerized goods, data structures, legal matters, etc. Mutually exclusive with Active Thing. See Appendix B and Appendix C.

Payment

A transfer of Sovrin Tokens or other cryptographically verifiable units of value from one Entity to another Entity.

Payment Address

The address of a Payment Transaction on the Sovrin Payment Ledger.

Payment Transaction

A Transaction with the Sovrin Payment Ledger that makes a Payment.

Peering

An N-wise relationship that does not need a separate Entity to coordinate. Compare Group.

Permissioned Write Access

The set of policies defined by the Sovrin Governance Framework governing how an Identity Owner may write a Transaction to the Sovrin Ledger using an authorized Transaction Endorser. Mutually exclusive with Public Write Access. See *Sovrin Ledger Access Policies*.

Persona

In the context of digital identity and user experience design, a fictional character created to represent a classification of an Individual that might use a site, brand, or product in a similar way.

Personal Data

As defined by the EU General Data Protection Regulation (GDPR), any information relating to an identified or identifiable natural person. In the GDPR, this natural person is called the Data Subject. In the Sovrin Governance Framework, this natural person is called an Individual.

Policy

A business, legal, or technical rule specified in a Governance Framework. In the Sovrin Governance Framework, a Policy is expressed using a “MUST”, “SHOULD”, “MAY”, “MUST NOT”, “SHOULD NOT”, or “MAY NOT” statement following the rules defined in IETF RFC 2119.

Practice

An actionable process that implements a Policy.

Privacy by Design

A set of seven foundational principles for taking privacy into account throughout the entire design and engineering of a system, product, or service. Originally defined by the Information and Privacy Commissioner of Ontario, Canada. Specific Sovrin Privacy by Design principles are a subset of the Core Principles in the Sovrin Governance Framework.

Private Data

Data over which an Entity exerts access control. In Sovrin Infrastructure, Private Data is never stored on the Sovrin Ledger. Private Data may be stored by an Agent in a Wallet or Vault or other secure location. Mutually exclusive with Public Data.

Private Key

The half of a cryptographic key pair designed to be kept as the Private Data of an Entity. In elliptic curve cryptography, a Private Key is called a signing key.

Procedure

A set of actionable steps that implements a Practice.

Proof

Cryptographic verification of a Claim or a Credential. A digital signature is a simple form of Proof. A cryptographic hash is also a form of Proof. Zero Knowledge Proofs enable selective disclosure of the information in a Credential. See Appendix G.

Proof Request

The data structure sent by a Verifier to a Holder that describes the Proof required by the Verifier. Proof Requests are sent and received using the Sovrin Protocol.

Prover

A role played by an Entity when it generates a Zero Knowledge Proof from a Credential. The Prover is also the Holder of the Credential. See Appendix G.

Pseudonym

A DID used to prevent correlation outside of a specific context. A Pseudonym may be Pairwise, N-wise, or Anywise. See also Anonym and Verinym.

Public Data

Data over which an Entity does not exert access control—it is publicly available to be read by anyone. In Sovrin Infrastructure, all Transactions on the Sovrin Ledger are Public Data. Mutually exclusive with Private Data.

Public Key

The half of a cryptographic key pair designed to be shared with other parties in order to decrypt or verify encrypted communications from an Entity. In digital signature schemes, a Public Key is also called a verification key. A Public Key may be either Public Data or Private Data depending on the policies of the Entity. In Sovrin Infrastructure, a Public Key is an Attribute of a Sovrin Entity. All Public Keys published on the Sovrin Ledger are Public Data.

Public Profile

In Sovrin Infrastructure, a Public Profile is a set of Attributes describing a Sovrin Entity, including its Legal Identity, logo(s) or other trademarks, location(s), marketing information, web links, and any other information that may be required by the Sovrin Governance Framework or a Domain-Specific

Governance Framework in order to ensure transparency and accountability.

Public Write Access

The set of policies defined by the Sovrin Governance Framework governing how an Identity Owner may write a Transaction directly to the Sovrin Ledger without needing to go through an authorized Transaction Endorser. Mutually exclusive with Permissioned Write Access. See *Sovrin Ledger Access Policies*.

Public Read Access

The set of policies defined by the Sovrin Governance Framework specifying the policies applying to read access to the Sovrin Ledger. See *Sovrin Ledger Access Policies*.

Purpose

The overarching goal of a Governance Framework as defined by its Governance Authority and Trust Community. The Purpose of Sovrin Infrastructure as a global public utility is defined in section 1 of the Sovrin Governance Framework.

Q

R

Recovery Key

A special Private Key used for purposes of recovering a Wallet after loss or compromise. In the DKMS key management protocol, a Recovery Key may be cryptographically sharded for secret sharing among multiple Trustees.

Recovery Key Trustee

A Trustee trusted by another Identity Owner to authorize sharing back a Recovery Key for purposes of restoring a Wallet after loss or compromise.

Relying Party

An Entity that consumes Identity Data and accepts some Level of Assurance from another Entity for some purpose. Verifiers are one type of Relying Party.

Resolver

A software module that accepts an Identifier as input, looks up the Identifier in a database or ledger, and returns metadata describing the identified Entity. The Domain Name System (DNS) uses a DNS resolver. Self-Sovereign Identity uses a DID Resolver.

Revocation

The act of an Issuer revoking the validity of a Claim or a Credential. With the Sovrin Protocol and the Sovrin Ledger, Revocation is accomplished using a Revocation Registry.

Revocation Registry

An online repository of data needed for Revocation. In Sovrin Infrastructure, a Revocation Registry is a privacy-respecting cryptographic data structure maintained on the Sovrin Ledger by an Issuer in order to support Revocation of a Credential. See Transaction Type.

Revocation Registry Definition

In Sovrin Infrastructure, the Transaction Type written by an Issuer to create a new Revocation Registry.

Revocation Registry Entry

In Sovrin Infrastructure, the Transaction Type written by an Issuer to update the state of a Revocation Registry. A Revocation Registry Entry may authorize newly issued Credentials or revoke previously issued Credentials.

S

Schema

A machine-readable definition of the semantics of a data structure. Schemas are used to define the Attributes used in one or more Credential Definitions.

Schema Overlay

Synonym for Overlay.

Security by Design

A widely recognized set of principles for building security into systems, products, and services from the very start. Specific Sovrin Security by Design principles are a subset of the Core Principles in the Sovrin Governance Framework.

Selective Disclosure

A Privacy by Design principle of revealing only the subset of the data described in a Claim, Credential, or other set of Private Data that is required by a Verifier. There are many techniques for achieving Selective Disclosure. One of the primary techniques used in Sovrin Infrastructure is Zero Knowledge Proof cryptography.

Self-Certification

The act of an Entity issuing a Self-Issued Credential that serves as a public Claim of conformance to a Governance Framework.

Self-Certification Credential

A Credential that asserts Self-Certification.

Self-Certification Page

A page on the website of the Issuer of a Self-Certification Credential that includes a link to the Credential and human-readable statement describing the Credential.

Self-Issued Credential

A Credential whose Holder is the Issuer of the Credential.

Self-Sovereign Identity

An identity system architecture based on the core principle that Identity Owners have the right to permanently control one or more Identifiers together with the usage of the associated Identity Data. The Sovrin Governance Framework specifies two types of Identity Owners: Independents, who do not need to rely on any external administrative authority; and Dependents, who need to rely on a Guardian.

Service Endpoint

An addressable network location offering a service operated on behalf of an Entity. As defined in the DID specification, a Service Endpoint is expressed as a URI (Uniform Resource Identifier). In the Sovrin Network, a Cloud Agent uses a specific type of Service Endpoint as specified by the Sovrin Protocol. See Appendix F.

SGF

Acronym for Sovrin Governance Framework.

Social Purpose Organization

An Organization whose primary mission is service to society rather than generation of profit.

Sovereign Domain

The set of Agents, Wallets, Vaults, devices, services, and other digital resources over which an Identity

Owner exercises sovereignty. Note that the actual sovereignty of the Identity Owner is limited to the degree such control is protected by the Developer of the hardware or software the Identity Owner is using.

Sovrin

The primary trademark of the Sovrin Foundation held in trust on behalf of the Sovrin Community.

Sovrin Board of Trustees

The set of Trustees entrusted with governance of the Sovrin Foundation under its current governance model. The responsibilities of the Sovrin Board of Trustees are specified in the Sovrin Governance Framework and its Controlled Documents.

Sovrin Builder Network (BuilderNet)

A non-authoritative version of the Sovrin Ledger deployed for the purposes of testing new versions of the Sovrin Open Source Code and preparing new Stewards for activation on the Sovrin Main Network. See also Sovrin Staging Network.

Sovrin Code

The Sovrin Open Source Code or any other computer code that is functionally equivalent.

Sovrin Code Repository

The official version control repository for Sovrin Open Source Code and other documents of the Sovrin Foundation as designated from time to time by the Sovrin Board of Trustees. At present, this is the GitHub repository at https://github.com/sovrin-foundation.

Sovrin Community

A specific Trust Community defined as the set of all Identity Owners cooperating under the Sovrin Governance Framework.

Sovrin Config Ledger

The subledger of the Sovrin Ledger used to record a special set of Transaction Types that are not publicly writable as they are reserved for configuration of the Sovrin Ledger. Writes to the Sovrin Config Ledger can only be made by Sovrin Trustees or their Delegates.

Sovrin Consensus Protocol

The Byzantine fault tolerant protocol used to communicate between Nodes to maintain the Sovrin Ledger. See the technical documentation for Hyperledger Indy.

Sovrin DID

A DID that conforms to the Sovrin DID Method Specification.

Sovrin DID Method Specification

A Controlled Document defined by the Sovrin Technical Governance Board specifying the format, registration, and resolution of DIDs rooted in the Sovrin Ledger or a Sovrin Microledger. The Sovrin DID Method Specification must conform to the requirements of a DID method specification as specified in the W3C DID specification.

Sovrin Domain Ledger

The subledger of the Sovrin Ledger used to record Identity-related Transaction Types except Payments (which use the Sovrin Payment Ledger). The Sovrin Domain Ledger is publicly readable. It is publicly writable via protection mechanisms specified in the Sovrin Governance Framework.

Sovrin Entity

A classification of an Entity that is described by Sovrin Identity Data including at least one Sovrin DID. A Sovrin Entity must be either an Identity Owner or a Thing. A Sovrin Entity may play the role of the Subject, Issuer, Holder, Prover, and/or Verifier of a Credential. Mutually exclusive with Other Entity.

Sovrin Foundation

The non-profit public trust organization chartered to administer Sovrin Infrastructure on behalf of the Sovrin Community. The Sovrin Foundation is the Governance Authority for the Sovrin Governance Framework and the Sovrin Web of Trust Framework. The Sovrin Foundation website is https://sovrin.org. See Appendix E.

Sovrin Glossary

An alphabetically sorted list of terms used in the Sovrin Governance Framework, each of which has a short description (definition) and optionally additional text that provides further explanation. The Sovrin Glossary (i.e. the present document) is a Controlled Document of the Sovrin Governance Framework.

Sovrin Governance Framework (SGF)

The Governance Framework defined by the Sovrin Foundation to govern Sovrin Infrastructure. The Sovrin Foundation is the Governance Authority for the Sovrin Governance Framework. The Sovrin Governance Framework consists of the Sovrin Governance Framework Master Document plus the Controlled Documents listed in Appendix A of the Master Document. The Sovrin Governance Framework is also referred to as the Sovrin Trust Framework.

Sovrin Governance Framework Master Document

The controlling document of the Sovrin Governance Framework. Appendix A of the Master Document lists the Controlled Documents that constitute the rest of the Sovrin Governance Framework.

Sovrin Governing Body

An official governing body within the Sovrin Foundation. The Sovrin Governance Framework Working Group is an example of a Sovrin Governing Body. The list of official *Sovrin Governing Bodies* is maintained as a Controlled Document of the Sovrin Governance Framework. See Appendix A of the Sovrin Governance Framework Master Document.

Sovrin Identity

The subset of Sovrin Identity Data shared by a Sovrin Entity in the context of a specific Connection (Pairwise) or publicly in the context of the Sovrin Ledger (Anywise). To respect privacy, a Sovrin Entity may have as many Sovrin Identities as needed to maintain their desired separation of contexts. See Appendix A.

Sovrin Identity Data

The collection of Identity Data, including DIDs, Public Keys, Attributes, Credentials, and Proofs, that describe a Sovrin Entity. See Appendix A.

Sovrin Infrastructure

A term encompassing all of the components that constitute Sovrin as a global public utility for Self-Sovereign Identity, including the Sovrin Ledger, Sovrin Network, Sovrin Web of Trust, Sovrin Governance Framework, and the Sovrin Foundation.

Sovrin Infrastructure Layers

The four layers of Sovrin Infrastructure: from bottom-to-top, the Sovrin Ledger Layer, the Agent-to-Agent Protocol Layer, the Credential Exchange Layer, and the Governance Framework Layer. See Appendix D.

Sovrin Infrastructure Roles

The business roles defined in the Sovrin Governance Framework for each of the four Sovrin Infrastructure Layers: Sovrin Ledger Layer Roles, Agent-to-Agent Protocol Layer Roles, Credential Exchange Layer Roles, and Governance Framework Layer Roles. See Appendix D.

Sovrin Ledger

The distributed, continuously-replicated global cryptographic database of Transactions maintained by Stewards operating Nodes communicating with the Sovrin Consensus Protocol. The Sovrin Ledger consists of four subledgers: the Sovrin Config Ledger, Sovrin Node Ledger, Sovrin Domain Ledger (also called the Sovrin Main Ledger), and Sovrin Payment Ledger. Only the Sovrin Domain Ledger and Sovrin Payment Ledger accept publicly available Transaction Types. See *Sovrin Ledger Access Policies* and Appendix E.

Sovrin Ledger Fee

The fee in fiat currency, Sovrin Tokens, or other units of economic value for making a write to the Sovrin Ledger. See *Sovrin Governing Bodies* for more information about the process of governing Sovrin Ledger Fees.

Sovrin Ledger Fee Table

A table of Sovrin Ledger Fees determined by the Sovrin Foundation and stored on the Sovrin Config Ledger.

Sovrin Ledger Layer

The first Sovrin Infrastructure Layer comprised of the Sovrin Ledger. See Appendix E.

Sovrin Ledger Layer Roles

The business roles defined at the Sovrin Ledger layer of Sovrin infrastructure. These include the Sovrin Foundation, Steward, Transaction Author, and Transaction Endorser. See Appendix E.

Sovrin Main Ledger

Synonym for Sovrin Domain Ledger.

Sovrin Main Network

The authoritative version of the Sovrin Ledger operated by Stewards hosting Validator Nodes. The Sovrin Main Network is separate from and complementary to the Sovrin Builder Network and the Sovrin Staging Network.

Sovrin Microledger

A Microledger that uses a Sovrin DID and conforms to the specifications for Sovrin Microledgers defined by the Sovrin Technical Governance Board. A Sovrin Microledger is separate (“off-ledger”) from the Sovrin Ledger, however future Transaction Types for the Sovrin Ledger may include special features to support Sovrin Microledgers.

Sovrin Network

The Sovrin Ledger and its Nodes plus the set of all Agents that communicate with the Sovrin Ledger and with each other using the Sovrin Protocol.

Sovrin Node Ledger

The subledger of the Sovrin Ledger used to record Transactions identifying the authorized Nodes. The Sovrin Node Ledger is publicly readable but not publicly writable; writes may only be made by Trustees or Stewards.

Sovrin Open Source Code

The computer code base governed by the Sovrin Technical Governance Board and distributed under an Open Source License to operate Nodes, Wallets, and Agents. The Sovrin Open Source Code is currently maintained primarily at the Hyperledger Indy Project managed by Linux Foundation and secondarily at the Sovrin Code Repository managed by the Sovrin Foundation.

Sovrin Payment Ledger

A subledger of the Sovrin Ledger used to record Payment Transactions. The Sovrin Payment Ledger is publicly readable. It shall be publicly writable under Public Write Access using Sovrin Ledger Fees as specified in the Sovrin Governance Framework.

Sovrin Principle

A governing principle of the Sovrin Community. The Core Principles are published in section 2 of the Sovrin Governance Framework.

Sovrin Protocol

The Open Standard Agent-to-Agent Protocol for communicating between Agents, performing Transactions with the Sovrin Ledger, performing Credential Exchange, or implementing other Interaction Patterns as defined by the Sovrin Community and implemented in the Sovrin Open Source Code. See Appendix F.

Sovrin Protocol Token

A cryptographic token that may be exchanged using the Sovrin Protocol via Transactions with the Sovrin Payment Ledger. The Sovrin Protocol Token implements specifications defined by the Sovrin Technical Governance Board and policies defined by the Sovrin Governance Framework.

Sovrin Provisional Trust Framework (SPTF)

The formal name for the first version of what is now the Sovrin Governance Framework. The SPTF was approved by the Sovrin Board of Trustees on 28 June 2017.

Sovrin Stack

Synonym for Sovrin Infrastructure Layers. See Appendix D.

Sovrin Staging Network (StagingNet)

A non-authoritative version of the Sovrin Ledger operated by Stewards for the purpose of demonstrating and verifying Sovrin-based solutions. Although it should run the same version of the Node software as the Sovrin Main Network, the Sovrin Staging Network is intended to remain relatively stable for long periods while the Sovrin Builder Network is used for active testing and may need to be frequently reset. The Sovrin Staging Network was previously known as the Sovrin TestNet.

Sovrin Steward Agreement

The legal contract between the Sovrin Foundation and a Steward. The Sovrin Steward Agreement incorporates the Sovrin Governance Framework and the Sovrin Glossary as appendices.

Sovrin Technical Governance Board (TGB)

The set of technical experts appointed by the Sovrin Foundation Board of Trustees to oversee the technical design and architecture of Sovrin Infrastructure. The TGB is one of the Sovrin Governing Bodies.

Sovrin Token

Synonym for Sovrin Protocol Token.

Sovrin Trust Assurance Framework

A Controlled Document of the Sovrin Governance Framework that defines criteria and processes for assessing conformance of Entities in Sovrin Infrastructure Roles, including the Sovrin Foundation itself, to the policies of the Sovrin Governance Framework. See Appendix A of the Sovrin Governance Framework Master Document and Appendix H.

Sovrin Trust Framework

Synonym for Sovrin Governance Framework. This was the term used for the first generation of the framework, formally known as the Sovrin Provisional Trust Framework.

Sovrin Trust Mark

A trademark, design mark, logo, icon, or other trust mark defined by the Sovrin Foundation for indicating conformance with the Sovrin Governance Framework. See *Sovrin Trust Mark Policies*.

Sovrin Trust Mark License

The license governing the use of a Sovrin Trust Mark as published on the Sovrin Foundation website.

See *Sovrin Trust Mark Policies*.

Sovrin Trustee

A Trustee who is a member of the Sovrin Foundation Board of Trustees. The trust in Sovrin Trustees is bestowed collectively on behalf of all Identity Owners.

Sovrin Web of Trust

The global network of interwoven Trust Communities implementing the Sovrin Web of Trust Model. See Appendix H.

Sovrin Web of Trust Governance Framework

The Domain-Specific Governance Framework defined by the Sovrin Foundation to implement the Sovrin Web of Trust Model by specifying Credentials, Credential Exchange, and Interaction Patterns for decentralized discovery, navigation, and verification of Domain-Specific Governance Frameworks, Trust Communities, and Trust Community Members. See Appendix H.

Sovrin Web of Trust Model

The decentralized, non-hierarchical trust model defined by the Sovrin Governance Framework, the Sovrin Web of Trust Framework, and the Sovrin Stack. The Sovrin Web of Trust Model does not rely on a single root of trust, but empowers any Sovrin Entity to serve as a root of trust and enables all Sovrin Entities to participate in any number of interwoven Trust Communities, either informally or as defined by Domain-Specific Governance Frameworks. See Appendix H.

SSI

Acronym for Self-Sovereign Identity.

SSI Network

A generic version of the Sovrin Network that supports the SSI Protocol and the SSI Stack. Using interoperable Open Standards and Governance Frameworks, multiple SSI Networks can work together to form a unified SSI Layer.

SSI Protocol

A generic version of the Sovrin Protocol that works at the second layer of the SSI Stack to enable Credential Exchange and Governance Frameworks to work interoperably across any number of SSI ledgers, blockchains, or networks.

SSI Stack

A generic version of the Sovrin Stack in which the bottom layer—the Sovrin Ledger layer—is expanded to include any distributed ledger, blockchain, or other SSI Network capable of supporting the three higher layers—the Agent-to-Agent Protocol layer, the Credential Exchange layer, and the Governance Framework layer.

State Proof

A Proof requested from a Node that provides cryptographic verification that the response reflects the current state of the Sovrin Ledger.

Steward

An Organization approved by the Sovrin Foundation to operate a Node. A Steward must meet the qualifications defined in the *Steward Business Policies* and the technical requirements defined in the *Steward Technical Policies* (see Appendix A of the Sovrin Governance Framework Master Document). A Steward must also execute the Sovrin Steward Agreement. See Appendix E.

Subject

The Entity whose Identifiers are asserted by DIDs and whose Attributes are asserted by Credentials. Aligns with the definitions provided by the W3C Credentials Community Group and W3C Verifiable Claims Working Group. See Appendix G.

T

TGB

Acronym for Sovrin Technical Governance Board.

Thing

An Entity that is not an Individual or an Organization and thus cannot be held legally accountable. A Thing may be a Natural Thing or a Man-Made Thing. In Self-Sovereign Identity, a Thing is represented by an Agent that can form Connections, exchange Credentials, and communicate securely even if the Thing itself is not network-enabled. Mutually exclusive with Identity Owner. To participate in an SSI ecosystem, every Thing must have a Thing Controller. NOTE: Not all objects are Things in the sense defined here. A Thing must be a uniquely identifiable Entity that is not fungible, i.e., not directly replaceable or exchangeable with another Thing. See Appendix B and Appendix C.

Thing Controller

A Controller that controls the Sovrin Identity Data, including the Private Keys, for a Thing. Every Thing must have a Thing Controller. The Thing Controller may or may not be the legal owner of the Thing, however the Thing Controller may still be legally responsible for actions Agent(s) take on behalf of the Thing. See Appendix C.

Thing Controller Credential

A Credential issued to a Thing Controller by an Identity Owner who has the legal authority to assign control of a Thing. A Thing Controller Credential may also be issued to a Thing if the Thing has its own Private Keys. See Appendix C.

Tombstone

A mark associated with a Transaction to suggest that the Transaction should no longer be returned in response to requests for read access. In the Sovrin Ledger, a Tombstone may be either a Node-Specific Tombstone or a Ledger-Wide Tombstone. Tombstones do not modify the Sovrin Ledger—only the behavior of a Node that serves data from the Ledger and that wishes to honor the Tombstone's semantics. In the general context of Self-Sovereign Identity, Tombstones are undesirable, as they represent a vector for censorship. However, they may be used by a specific Steward that is forced to comply with a legal demand to stop returning a specific Transaction, such as a Transaction containing data that is locally considered Personal Data or that is illegal or violates the Transaction Author Agreement in some other way. In such a case, other Stewards may not face the same legal demands and may take different action.

Transaction

A record of any type written to the Sovrin Ledger. Transactions are classified by Transaction Type.

Transaction Author

The Entity initiating a Transaction. Most (but not all) Transaction Authors will be Identity Owners. In Sovrin infrastructure, Transaction Authors must sign the Transaction Author Agreement. See also Transaction Endorser. See Appendix E.

Transaction Author Agreement

A Controlled Document which functions as the legal agreement between the Sovrin Foundation and any Transaction Author which must be digitally signed or otherwise explicitly agreed to by the Transaction Author in order to write a Transaction. See *Sovrin Ledger Access Policies* and Appendix E.

Transaction Data

The set of data and metadata processed by a Node in order to validate and write a Transaction.

Transaction Endorser

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. See Appendix E.

Transaction Endorser Agreement

A Controlled Document which functions as the legal agreement between the Sovrin Foundation and any Transaction Endorser. See *Sovrin Ledger Access Policies* and Appendix E.

Transaction Type

A classification of a Transaction. Authorized Transaction Types are specified by the Sovrin Technical Governance Board in the *Steward Technical Policies* (see Appendix A of the Sovrin Governance Framework Master Document). For example supported Transaction Types for the Sovrin Main Ledger include: NYM (for writing a DID), ATTRIB (for writing an Attribute), CLAIM_DEF (for writing a Credential Definition), SCHEMA (for writing a Schema), REVOC_REG_DEF (for writing a Revocation Registry Definition), and REVOC_REG_ENTRY (for writing a Revocation Registry Entry).

Trust Anchor

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. *(Note: In the Sovrin Provisional Trust Framework, this term was used to describe what is now defined as a Transaction Endorser. That usage is now deprecated.)* See Appendix H.

Trust Anchor Credential

A Credential issued by a Governance Authority or an Auditor asserting that an Issuer is Accredited to serve as a Trust Anchor. See Appendix H.

Trust Assurance

A means by which one Entity conveys confidence that another Entity is complying with the rules of a Governance Framework. See the *Sovrin Trust Assurance Framework*.

Trust Community

A set of Entities cooperating to achieve their mutual trust objectives. An informal Trust Community may not have an official structure or a Governance Framework. A formal Trust Community consists of the set of all Entities participating in a Governance Framework. See also Sovrin Community.

Trust Community Member

An Entity who has agreed to participate in a Trust Community. Participation may be informal, such as via a terms of service agreement or other mechanism; or formal, such as via a legal contract or membership agreement, or both. The Sovrin Community is both an informal and a formal Trust Community governed by the Sovrin Governance Framework.

Trust Framework

Synonym for Governance Framework, particularly when used in the context of digital identity systems.

Trustee

An Identity Owner entrusted with specific identity control responsibilities by another Identity Owner or with specific governance responsibilities by a Governance Framework. See Recovery Key Trustee and Sovrin Trustee. See Appendix C.

Trusteeship

A special form of Guardianship in which a Trustee is appointed by an Identity Owner to serve as a Guardian under specific circumstances, such as illness, incapacitation, or death. See Appendix C.

U

Unaccredited

The status of an Entity not being Accredited.

V

Validator Node

A Node that validates new Transactions and writes valid Transactions to the Sovrin Ledger using the Sovrin Consensus Protocol. A Node may be able to operate as either a Validator Node or an Observer Node, but at any one point in time it must operate in only one of these two roles. A Steward may run only one Validator Node on the Sovrin Main Network.

Vault

A term used to describe cryptographically-protected secure storage that is outside a Wallet but still accessible to and/or managed by an Agent. A Vault may (but is not required to) contain a Wallet. A Vault is often used for secure storage of digital assets too large to fit into a Wallet. Encryption and decryption of the contents of the Vault is usually performed by an Agent using Private Keys stored in a Wallet.

Verifiable Credential

A Credential that includes a Proof from the Issuer. Typically this proof is in the form of a digital signature. In Sovrin Infrastructure, a Verifiable Credential uses Zero Knowledge Proofs by default and can usually be verified by the Issuer Public Key stored in the Credential Definition on the Sovrin Ledger. Based on the definition provided by the W3C Verifiable Claims Working Group. See Appendix G.

Verifier

An Entity who requests a Credential or Proof from a Holder and verifies it in order to make a trust decision about a Sovrin Entity. Based on the definition provided by the W3C Verifiable Claims Working Group. See also Relying Party.

Verinym

A DID that it is directly or indirectly associated with the Legal Identity of the Identity Owner. Mutually exclusive with Anonym and Pseudonym.

Virtual Vault

The collection of all Vaults used by an Entity. For example, the Virtual Vault for an Individual Identity Owner would include the Vaults on all that person's devices, plus any cloud-based Vaults that are accessible to and/or managed by the Identity Owner's Agent(s). See also Sovereign Domain.

W

Wallet

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. In Sovrin infrastructure, Wallets implement the emerging DKMS standards for interoperable decentralized cryptographic key management.

Web of Trust

See Sovrin Web of Trust Model.

X

Y

Z

Zero Knowledge Proof
A Proof that uses special cryptography and a Link Secret to support Selective Disclosure of information about a set of Claims from a set of Credentials. A Zero Knowledge Proof provides cryptographic proof about some or all of the data in a set of Credentials without revealing the actual data or any additional information, including the Identity of the Prover.

Introduction to Appendices

— Informative —

The following appendices are intended to help readers understand core terms in the Sovrin Glossary in a more natural expository format than is possible in a pure alphabetical listing. **This content is *non-normative*, i.e., it is informative content only and does not modify the formal definition of any term provided in the Glossary.**

Eight appendices are provided as summarized in this table:

#	Appendix Name	Covers
A	**Sovrin Entities, Identities, and Connections**	The core concepts at the heart of Self-Sovereign Identity—and why SSI is inherently contextual
B	**Taxonomy of Entities**	The basic hierarchy of Entity types and how this taxonomy applies to SGF Policies
C	**Delegates, Guardians, and Controllers**	The three roles Identity Owners may play to help administer or control other Sovrin Identities
D	**Sovrin Infrastructure Layers**	The four layers of Sovrin Infrastructure (Sovrin Ledger, Agent-to-Agent Protocol, Credential Exchange, and Governance Framework)
E	**Sovrin Ledger Layer Roles**	The roles of the Sovrin Foundation, Steward, Transaction Author, and Transaction Endorser
F	**Agent-to-Agent Protocol Layer Roles**	The two types of Agents (Edge and Cloud) and the roles of Identity Owner, Agency, and Developer
G	**Credential Exchange Layer Roles**	The roles of Subject, Issuer, Holder/Prover, Verifier, and Insurer
H	**Governance Framework Layer Roles**	The roles of Trust Anchor, Credential Registry, Governance Authority, Auditor, and Auditor Accreditor

Appendix A: Sovrin Entities, Identities, and Connections

— Informative —

Figure A is a concept map of the core terms at the heart of the Sovrin Governance Framework.[1] Blue boxes represent the real-world starting points for Self-Sovereign Identity. Green boxes represent the core concepts defining Self-Sovereign Identity relationships. Orange boxes are the supporting data structures and repositories required to generate, describe, and prove Sovrin Identities.

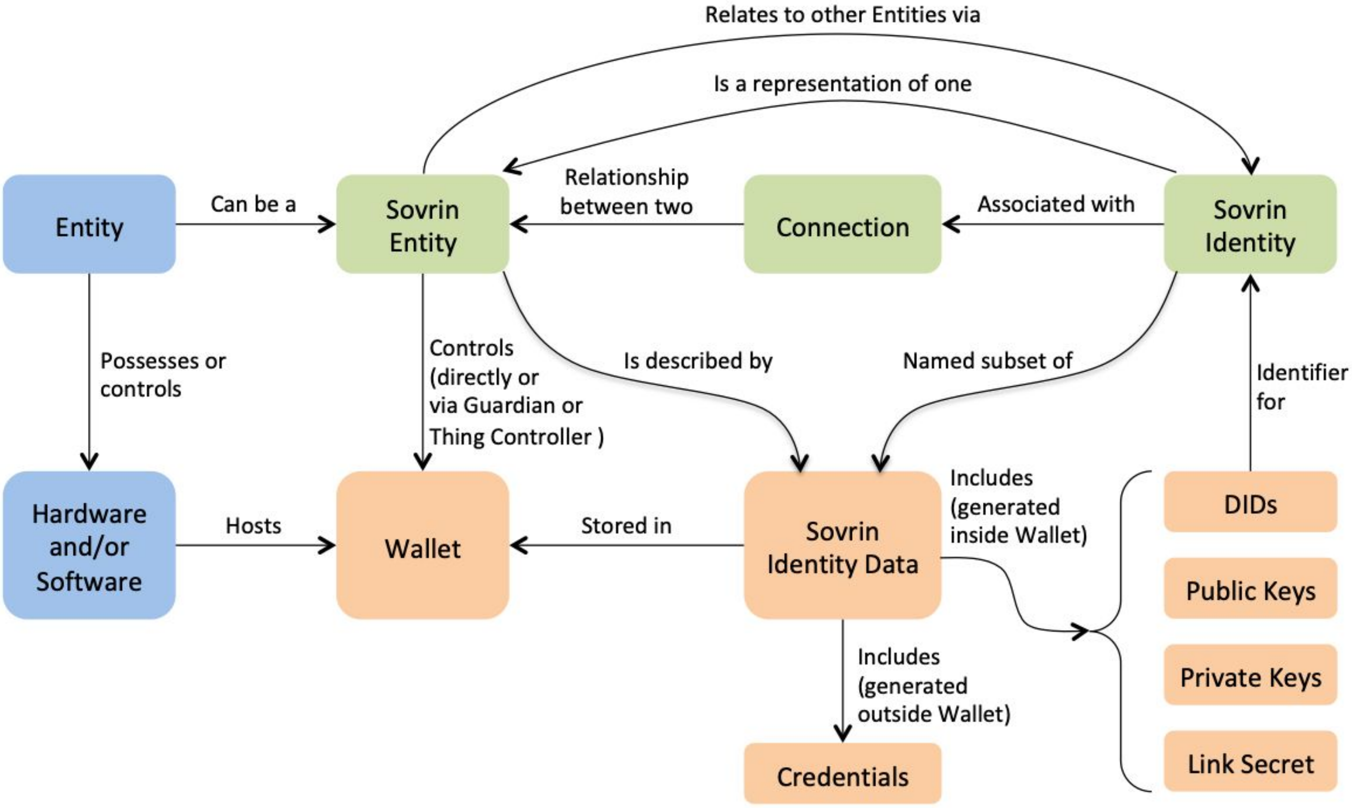

Figure A: Core concepts defining Sovrin Identity relationships

An **Entity** of any type (see Appendix B) becomes a **Sovrin Entity** as soon as it generates and shares at least one **Sovrin Identity**. Each Sovrin Identity consists of exactly one **DID** (Decentralized Identifier), at least one pair of **Public and Private Keys** (only the Public Key is shared), and exactly

[1] Special thanks to Andrew Hughes for leading the development of this concept map.

one associated **Link Secret** (which is never shared directly but only used to produce Zero Knowledge Proofs). In the vast majority of cases it will also consist of one or more **Credentials** (which in Sovrin Infrastructure are also not shared directly, only via Proofs).

Collectively, these components are called **Sovrin Identity Data** and are stored in a **Wallet** under the control of either: a) the Identity Owner (or his/her Delegate or Guardian—see Appendix C), or b) a Thing Controller in the case of a Thing (see Appendix C). Note that this Wallet may be stored on a local device accessed by an Edge Agent, or it may be stored in the cloud and accessed by a Cloud Agent (see Appendix F).

By default a Sovrin Identity is Private Data, i.e., the DID and Public Key are generated in the context of a specific **Connection** with another Sovrin Entity and only shared over that Connection. This form of Sovrin Identity is called **Pairwise Pseudonymous**; it is not registered with the Sovrin Ledger but is known only to the two parties to a Connection.

Every Sovrin Entity also has the right to register a Sovrin Identity as Public Data.[2] This form of Sovrin Identity is not contextual to a specific Connection; rather an **Anywise** DID is registered with the Sovrin Ledger so that anyone may discover and verify the Public Key(s), Service Endpoints, and other Sovrin Identity Data associated with this Sovrin Identity. An Anywise Sovrin Identity is most often needed by Issuers who need their Credentials to be publicly verifiable.

In summary, a Sovrin Identity always consists of a “package” (subset) of the Sovrin Identity Data that describes the identified Sovrin Entity. This package is shared either privately over a specific Connection (Pairwise) or publicly with the world (Anywise). What makes it self-sovereign is that the Sovrin Entity always controls:

1. **What is shared**—the contents of the package.
2. **When and where it is shared**—the context of the package.
3. **Who can access it**—the keys for encrypting and signing the package if it is not Public Data.

[2] This option is not currently available to Individuals under the SGF V2 due to regulatory uncertainty about the applicability of GDPR to DIDs registered by individuals on public ledgers. See the Preamble to *Sovrin Ledger Access Policies*.

Appendix B: Taxonomy of Entities

— Informative —

Figure B is a taxonomy of the different types of Entities defined in the SGF. Each Entity type is defined for the purpose of describing principles and policies that apply only to that distinct type of Entity. Some are business distinctions; some are legal distinctions; some are technical distinctions. This appendix explains the rationale for each branch in this taxonomy tree.

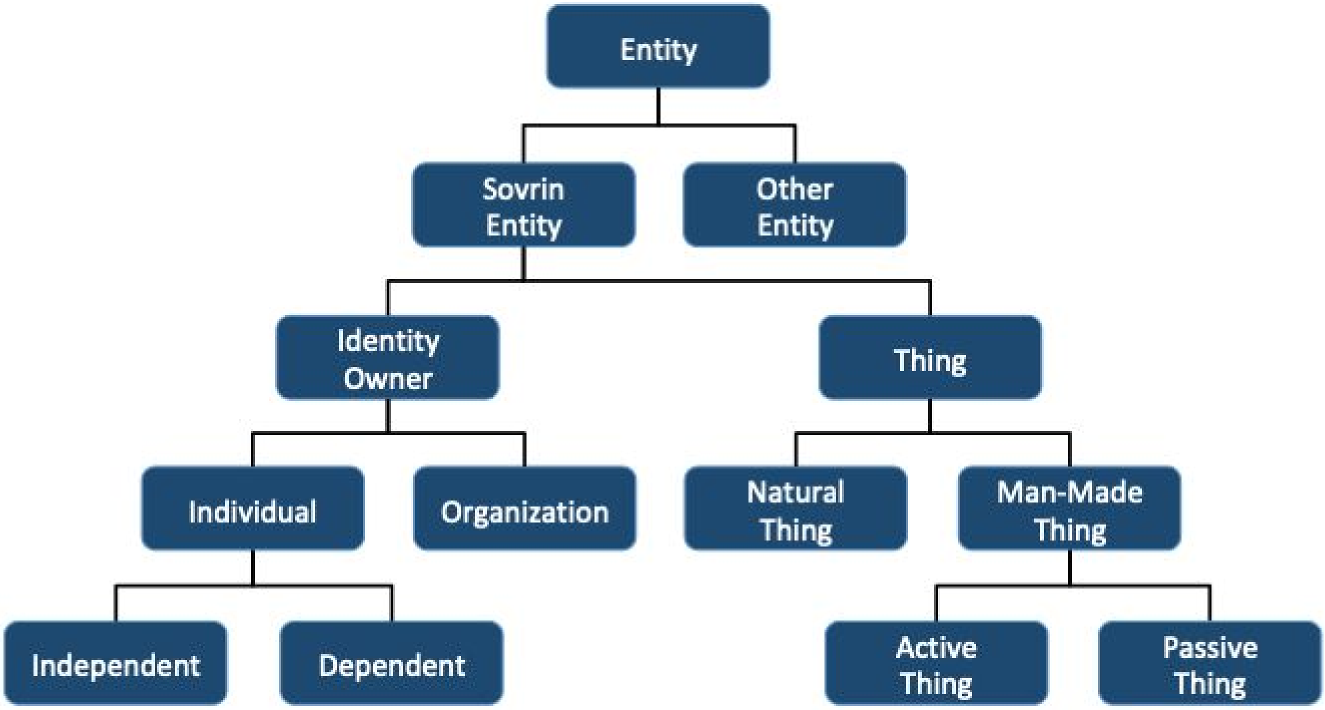

Figure B: Taxonomy of Entities defined in the Sovrin Governance Framework

Note that this is a strict type tree, i.e., in the context of a particular Connection at a particular point in time, an Entity falls into exactly one of these classifications. Each class inherits the attributes of all parent classes in that branch. For example, an Independent is a type of Individual, an individual is a type of Identity Owner, an Identity Owner is a type of Sovrin Entity, and a Sovrin Entity is a type of Entity.

The root class of **Entities** is subclassified into **Sovrin Entities** and **Other Entities**. Sovrin Entities have at least one Sovrin Identity (and thus at least one Sovrin DID). Other Entities are identified in some other identity system. Note that the Sovrin Network is designed to be as interoperable with as many other identity systems as possible, so Sovrin Entities are interoperable with all types of Entities.

Sovrin Entities are subclassified into **Identity Owners** and **Things**. The crucial distinction here is *legal accountability*. Identity Owners are Entities who have a right to Self-Sovereign Identity and can, under the appropriate circumstances, be held legally accountable for their interactions in the Sovrin Network. However, as noted in the Sovrin Glossary definition of Identity Owner:

> *"...the actual legal accountability of an Identity Owner for any particular action depends on many contextual factors including the laws of the applicable Jurisdiction, Guardianship, and so forth."*

Things are by definition Entities who are *not* capable of legal accountability no matter what the circumstances. This is why a Thing always requires a Thing Controller (see Appendix C). Things are subclassified into **Natural Things** and **Man-Made Things**. Natural Things are anything occurring in the natural world that are not the subject of human rights but which may have some degree of natural rights recognized in different legal Jurisdictions. Examples include animals, pets, plants, mountains, rivers, etc.

By contrast, a Man-Made Thing is distinguished by not having any natural rights under the law. Man-Made Things are subclassified into **Active Things** and **Passive Things** based on their capacity to hold their own Private Keys in their own Wallet and operate their own Agent. Active Things have this capacity—examples include computing devices, drones, robots, vehicles, satellites, etc. Passive Things do not have this capacity—examples include documents, books, non-computerized goods, software programs, files, data structures, legal matters, intellectual property, digital music, digital designs, etc.

Self-sovereign **Identity Owners** are subclassified into **Individuals** and **Organizations**. Individuals are natural persons—a legal concept widely recognized across jurisdictions. Organizations are any other type of legal person besides a natural person—for example a corporation, partnership, LLC (Limited Liability Corporation), government or governmental agency, NGO (Non-Governmental Organization), etc. Note that while both Individuals and Organizations can potentially be held legally responsible for actions, only Individuals actually take such actions in the real world. Organizations are abstract Entities whose actions are always taken indirectly by Individuals (or Things controlled by Individuals) acting as Delegates on their behalf.

Lastly, **Individuals** are subclassified into **Independents** and **Dependents**. In the context of a specific Connection at a specific point in time, an Individual is acting either as an Independent—a natural person who has direct control of the Private Key(s), Wallet(s), and Agent(s) needed to administer Sovrin Identities—or as a Dependent—a natural person who is not in a position to directly control their Private Key(s), Wallet(s), and Agent(s), either because of legal or physical incapability (such as a child or elderly parent), economic or political incapability (such as a refugee), or computing or networking incapability (such as not having a device or online access).

The distinction is particularly important because control of an owner's Private Keys is what makes an Identity Owner truly self-sovereign. However, a Dependent can still achieve self-sovereignty through use of a Guardian as explained in Appendix C.

Appendix C: Delegates, Guardians, and Controllers

— Informative —

The Sovrin Glossary defines three types of **identity control relationships**—relationships in which an Identity Owner exerts control on behalf of another Entity. The terms for these relationships and their associated roles are summarized in Figure C.

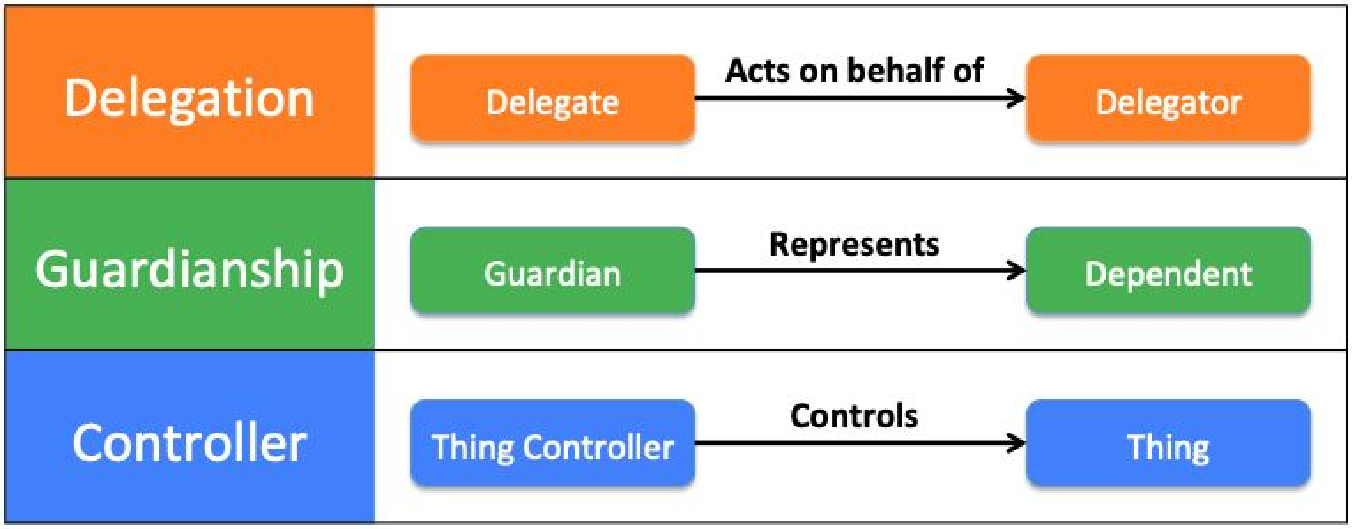

Figure C: The three types of identity control relationships defined in the Sovrin Glossary

Experience with these topics has taught the SGFWG that *these terms are closely related and easily confused*. The goal of this appendix is to explain the key distinctions summarized in Table 1.

	Delegation Relationship	Guardianship Relationship	Controller Relationship
Exists between two Identity Owners	Yes	Yes	No
Exists between an Identity Owner and a Thing	No	No*	Yes
Both parties control	Yes	No**	No***

their own Private Keys			
Who authorizes the relationship	Delegator	Dependent or a legal representative of the Dependent	Thing Controller (or legal owner of the Thing)
Authorization mechanism	Delegation Credential (may be backed by legal agreement)	Legal agreement (may be backed by Guardianship Credential)	Thing Controller Credential
Who has legal responsibility	Depends on the relationship (see text)	Guardian (serving as information fiduciary)	Depends on the relationship (see text)

* Although the strict definition of Guardianship in the Sovrin Glossary is confined to human Dependents, in a more general sense the term can also be applied to guardianship of Natural Things.

** A Dependent in one context may be an Independent in another context

*** Active Things have Private Keys and Agents but they are still under the control of the Thing Controller

Table 1: Primary distinctions between the three types of identity control relationships

Delegation Relationships (Delegate Acts on Behalf of an Delegator)

Delegation is perhaps the most common of all identity control relationships. People constantly delegate responsibilities to other people; organizational structures exist largely to define delegation relationships. The key to defining Delegation in the Sovrin ecosystem is that **it exists only between two Independent Identity Owners who both have direct control of their Private Keys**. If one Identity Owner does not control their Private Keys, it requires **Guardianship**; if one of the Entities is a Thing, it requires a **Controller**.[3]

Since Delegation requires both Identity Owners to control their own Private Keys (and thus have their own Wallets and Agents), a Delegation relationship can be authorized using a special type of Credential called a **Delegation Credential**. A Delegation Credential is issued to the Delegate by the Delegator. As the Holder of the Delegation Credential, the Delegate can then use the Sovrin

[3] A Guardian, who **must** itself be an Independent Identity Owner, can perform Delegation on behalf of Dependent. Likewise a Thing Controller can perform Delegation on behalf of a Thing.

Protocol to show a Proof to a Verifier that the Delegate is authorized to act on behalf of the Delegator with regard to some specific responsibility or capability.[4]

Common examples:

- A parent (Delegator) issuing a Delegation Credential to a babysitter (Delegate) to authorize him to approve medical treatment of a child in case of an emergency.
- A company (Delegator) issuing a Delegation Credential to an employee (Delegate) to authorize her to represent the company in a consortia or other external organization.
- A political party (Delegator) issuing a Delegation Credential to a party member (Delegate) to represent the party at a political convention or to vote on a ballot (e.g. the U.S. Electoral College).

The legal responsibility of a Delegate depends on the relationship with the Delegator and the duties being delegated. In some cases it may be strictly informal, such as one friend delegating to another the ability to unlock his garage door to borrow his power tools. In other cases, such as medical or legal authorizations, the legal responsibilities may be defined by existing law. In still other cases the Delegation Credential may explicitly reference an associated legal agreement defining liability and other legal considerations.

Guardianship Relationships (Guardian Represents a Dependent)

While Guardianship may not be as common as Delegation, it is vital to Sovrin infrastructure because it is the mechanism by which Self-Sovereign Identity can be extended to Dependents. As shown in Figure B in Appendix B, these are Individuals who are **not** in a position to directly control their Private Keys via the use of an Edge Agent on a local device.

This is the core distinction between Delegation and Guardianship: with the former, both Identity Owners control their own Private Keys. With the latter, the Guardian controls **two sets** of Private Keys—one for themselves, and one for the Dependent.

This means the Guardian literally acts online as the digital representative of the Dependent. In fact, for privacy reasons, it should be possible for a Dependent to control whether it is discoverable (without the Dependent's *and* the Guardian's permission) that a Dependent is represented by a Guardian.

[4] The technical specifications for interoperable Delegation Credentials have not yet been developed by the W3C Verifiable Claims Working Group, the Sovrin Foundation, or Hyperledger Indy; however, work is ongoing.

This of course requires very high degree of trust between the Dependent and the Guardian—trust that must be rooted in an offline legal relationship (whether a formal legal agreement or informally under natural law) because by definition the Dependent **cannot** assert it cryptographically using a Credential. This form of legal responsibility is known as an information fiduciary, and it is one of the most important new areas of law associated with Self-Sovereign Identity because it is a means of extending Self-Sovereign Identity to the more than 1.1 billion people who do not currently have any form of legal identity.

In some cases an Individual (such as a parent or spouse) or an Organization (such as a government, court, or NGO) may be in a position as an Identity Owner to authorize a Guardian to represent a Dependent. In that case, this Individual or Organization may issue a **Guardianship Credential** to the Guardian. With the appropriate permissions, the Guardian may then generate a Proof to a Verifier that the Guardian is authorized to represent the Dependent.

Common examples of Guardianship relationships include:

- A parent acting as a Guardian for a child (Dependent) until the child reaches the age of majority. This is an example where the parent may not have any Guardianship Credential (unless such a Credential is Self-Issued by the parent).
- An adult son or daughter acting as a Guardian for an aging parent (Dependent). In this case the son or daughter might have a Guardianship Credential issued by a court order, government agency, or other legal authority.
- A government agency acting as a Guardian for a homeless person (Dependent).
- An NGO acting as a Guardian for a refugee (Dependent).

When the Guardian is an Organization, the Organization will typically act as a Delegator to issue Delegation Credentials to its staff as Delegates to perform the actual functions of Guardianship on behalf of a Dependent. For example, an NGO that works with refugees in a developing country will issue Delegation Credentials to its staff working in the actual refugee camps. These staff members can now interact directly with refugees as Dependents, helping them take actions such as obtaining or proving Credentials for health care, immunizations, education, employment, etc.

The Sovrin Governance Framework asserts that every human Dependent has the right to become an Independent if and when they have the capability, capacity, and desire to directly control their own Private Keys—and that the Guardian must support this right. For example, a refugee who repatriates to another country where he/she is able to obtain a smartphone and Internet access can request to take control of his/her Wallet and thereby gain the complete self-sovereignty of an Independent. In the case of a person who was placed under Guardianship (e.g., by a court order), there also needs to be a process allowing that person to take back control (i.e., transitioning back to an Independent), assuming the necessary requirements have been met (e.g., court order returning power of attorney).

Trusteeship is a special form of Guardianship in which a Trustee is appointed by an Identity Owner to serve as a Guardian only under special circumstances, such as illness, incapacitation, or death. Trusteeship is vital to Self-Sovereign Identity management of digital estates.

> ***Note:*** *For legal precision, the term* ***Guardian*** *in the Sovrin Glossary is limited to guardianship of human Dependents. However the natural language term "guardian" can also be applied to many types of Natural Things as "dependents", particularly pets, livestock, or other animals who are dependent on humans but do not have the capacity to control their own Private Keys. The same goes for rivers, parks, or other natural monuments that require human protection. The primary difference between Natural Things as "dependents" and humans as Dependents is that only the latter have the capacity to become Independent. Thus Natural Things still require a Thing Controller to be responsible for their Private Keys.*

Digital Guardianship is such an important new area that the Sovrin Foundation is leading several initiatives in this space:

1. The SGFWG formed a Guardianship Task Force to further develop policy recommendations and governance models for Guardians.
2. The Sovrin Foundation formed the Global Policy Working Group to develop policy recommendations on SSI legal topics such as Guardianship and information fiduciaries.
3. The Sovrin Foundation chartered the Identity for All Council to support the development of identification systems that serve marginalized or otherwise underserved populations worldwide, with a focus on the highest need cases of the Global South.

Controller Relationships (Thing Controller Controls a Thing)

A Controller relationship is the easiest one to define: it only exists between an Identity Owner and a Thing. This role is called Thing Controller because the Identity Owner completely controls the Private Key(s), Wallet(s), and Agent(s) acting on behalf of the Thing.

All Things must have a Thing Controller because by definition a Thing cannot take legal responsibility for the actions of its Agent(s). This is true even in the case of Natural Things such as animals—while they may have their own natural rights (and thus may more naturally be thought of as needing "guardianship"), they cannot control their own Private Key(s), Wallet(s), and Agent(s).

With Man-Made Things, the Thing Controller relationship depends on the type:

1. **Passive Things cannot have their own Private Keys** and therefore require a Thing Controller to manage their Private Key(s), Wallet(s), and Agent(s). This is very much like the relationship of a Guardian to a Dependent except the Thing has no right to self-sovereignty (i.e., to become an Independent). This applies to any Thing that is not connected to a network or cannot send, receive, and process messages.
2. **Active Things can have their own Private Keys.** Active Things must be computing devices of some kind capable of connecting to a network, with their own Private Key(s) and Wallet(s) (even if minimal). They must also operate their own Agent(s) speaking at least a subset of the Sovrin Protocol.

Examples of Passive Things:

1. Inanimate physical objects such as manufactured goods, shipping containers, buildings, and machine parts.
2. Digital objects such as files, graphics, ontologies, and data structures.
3. Business documents such as purchase orders, invoices, waybills, and shipping receipts.

Examples of Active Things:

1. Computing devices used by Identity Owners (e.g., smartphones, laptops, desktops, servers, printers, smart TVs, smart cars, smart watches, etc.).[5]
2. Smart sensors used in manufacturing, shipping, transportation, etc.
3. Drones, robots, autonomous cars, and other computing devices capable of movement.

A critical point is that, even in the second case when the Thing has its own keys, **the Thing Controller is always in ultimate control of the Thing**. Without diving deep into Blade Runner-style arguments about AI (Artificial Intelligence) and free will, the actions of the Thing are always the responsibility—practically, legally, or ethically—of the Individual or Organization acting as the Thing Controller.

[5] The Agent for a Thing is **never** the same as the Agent for an Identity Owner using the Thing. Agents always represent Sovrin Identities, and a Sovrin Identity for the Thing is never the same as a Sovrin Identity for the Identity Owner.

So how does a Thing assert who its Thing Controller is—or a Thing Controller assert that it controls a Thing? While this can always be done offline either informally or with a legal agreement of some kind, it can also be done online using a **Thing Controller Credential**. Again, there are two cases:

1. **Passive Things.** In this case only the Thing Controller can hold a Thing Controller Credential. It may be Self-Issued, for example when the Thing Controller legally owns the Thing (e.g., a lawnmower), or it may be issued by a third party with legal authority over the Thing (e.g., a shipper issuing a Thing Controller Credential for a shipping container to a trucking company).
2. **Active Things.** In this case a Thing Controller Credential can also be issued to the Thing so it can generate a Proof of its Thing Controller. For example, both the company owning a drone and the drone itself could be issued a Thing Controller Credential by a governmental licensing agency. If the drone was lost or involved in an accident, both the company and the drone could prove who was the Thing Controller.

Note that while in some cases the Thing Controller may also be the legal owner of the Thing as personal or corporate property, a Thing Controller relationship alone does not assert ownership. The question of a Thing Controller's legal responsibility for the actions of the Thing depends on the type of Thing and the nature of the control relationship.

Appendix D: Sovrin Infrastructure Layers

— Informative —

Figure D graphically depicts the four layers of Sovrin Infrastructure—called the Sovrin Stack. This appendix will explain the overall purpose of each of these four layers; Appendices E, F, G, and H will explain the Sovrin Infrastructure Layer Roles and interactions that the Sovrin Governance Framework defines at each of these four layers.

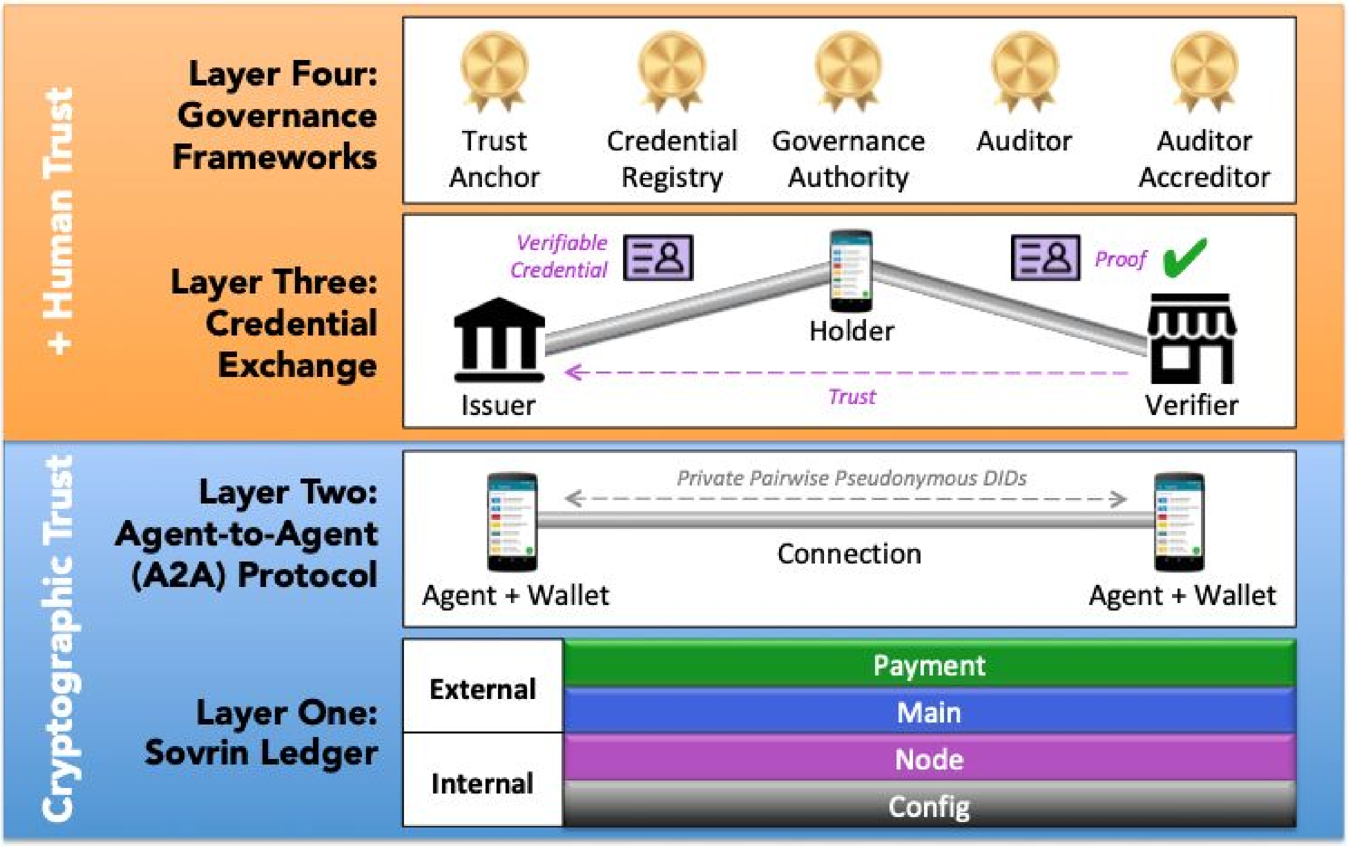

Figure D: The Four Layers of Sovrin infrastructure

The Sovrin Ledger Layer

The bottom layer—literally the foundation of Sovrin Infrastructure—is the Sovrin Ledger layer where public Sovrin Identities are rooted in Anywise DIDs. As described in Appendix A, Sovrin Identities typically only need to be rooted at this layer by Issuers who need their Credentials to be publicly verifiable. The Sovrin Ledger also includes publicly available Schemas, Credential Definitions, and Revocation Registries. Sovrin Ledger Layer Roles are described in Appendix E.

While the Sovrin Foundation governs one specific ledger—the Sovrin Ledger—at this layer, a generic version of Sovrin Infrastructure, called the **SSI Stack**, can run on top of any distributed ledger or blockchain that supports the three higher layers. This is the path to a globally interoperable SSI “network of networks” in which an Anywise DID can be rooted in any participating ledger, blockchain, or other decentralized network.

The Agent-to-Agent Protocol Layer

From both a privacy and scalability standpoint, it is critical that Sovrin Entities (Individuals, Organizations, Things) be able to form Connections, maintain Wallets, and exchange Credentials over direct, off-ledger peer-to-peer relationships. This is the job of the Agent-to-Agent (A2A) Protocol layer. Agent-to-Agent Protocol Layer Roles are described in Appendix F.

The specific A2A protocol features required by Sovrin Infrastructure are called the **Sovrin Protocol**. A more generic version of the Sovrin Protocol that operates across any SSI Network supporting the SSI Stack is called the **SSI Protocol**.

The Credential Exchange Layer

Taken together, the Sovrin Ledger layer and the Agent-to-Agent Protocol layer only establish **Cryptographic Trust**—trust that a set of machines (Man-Made Things) operating cryptographic algorithms will behave as expected. It does not establish **Human Trust**—trust that a set of people (Individuals and/or Organizations) will behave as expected.

This is the job of the next two layers, starting with the Credential Exchange layer. This is the layer where **Issuers** issue **Credentials** (describing **Subjects**) to **Holders** (which may or may not be the Subject). **Holders** then act as **Provers** to present **Proofs** of those Credentials to **Verifiers**, who use the Sovrin Ledger to look up the Issuer’s DID to get the Public Key needed to verify the Proof. Credential Exchange Layer Roles are described in more detail in Appendix G.

The Governance Framework Layer

Some Credentials are very narrow in scope—issued by a single Issuer and only accepted by that same Entity or a limited group of Entities acting as Verifiers. An example might be a coffee shop loyalty card. However many Credentials are intended for broader adoption—for example, birth certificates, passports, driving licenses, credit cards, diplomas, and vaccination records. These typically have multiple Issuers and any number—even a mass market—of Verifiers. Establishing

Human Trust in these widely-used credentials requires developing business and legal agreements between Issuers—typically a group of Organizations such as credit unions, banks, stores, healthcare providers, universities, or governments. This is the job of **Governance Frameworks**. Governance Framework Layer Roles are described in more detail in Appendix H.

Appendix E: Sovrin Ledger Layer Roles

— Informative —

Figure E is a visual depiction of the four roles at the Sovrin Ledger Layer—the bottom layer of the four layers of Sovrin Infrastructure covered in Appendix D. This appendix will explain how each of these four roles relate to the other.

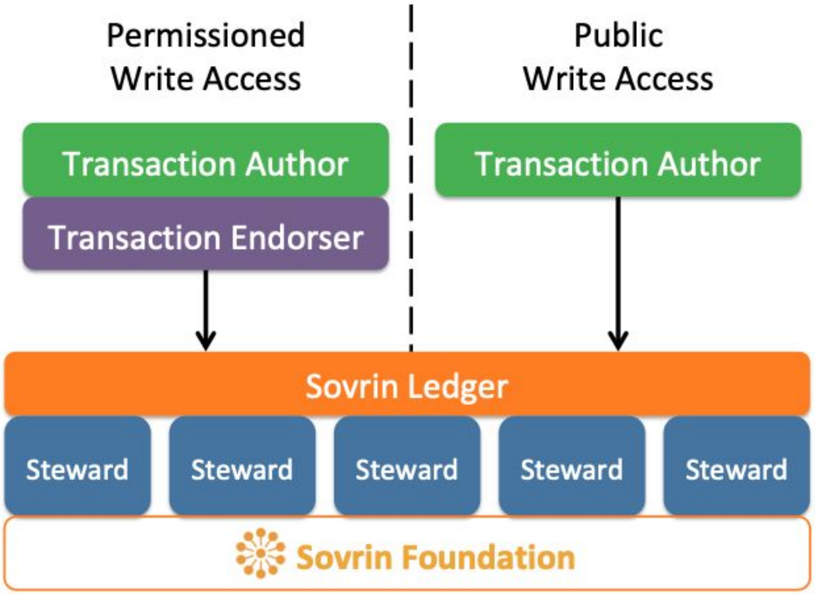

Figure E: Sovrin Ledger Layer Roles

The Sovrin Foundation

This is the non-profit public trust organization launched in September 2016 to establish Sovrin as a global public utility for self-sovereign identity. The Sovrin Foundation does not own or run the Sovrin Ledger—that is the collective job of the Sovrin Stewards (below). Rather, the job of the Foundation is to put in place the governance necessary for a decentralized network dedicated to SSI.

The vehicle for that governance is the Sovrin Governance Framework, which is why the Sovrin Governance Framework Working Group was one of the first Sovrin Governing Bodies. There are now eight of them that manage all aspects of Sovrin governance—see Appendix A of the Sovrin Governance Framework Master Document for the complete list. As discussed in Appendix H, the

Sovrin Foundation formally serves as the Governance Authority for the Sovrin Governance Framework.

The Sovrin Foundation collectively represents all Identity Owners who use (or wish to use) the Sovrin Network. The Foundation itself is ultimately governed by a set of Sovrin Trustees—Individuals from around the world with backgrounds in digital identity, security, privacy, governance, and public policy. Sovrin Trustees each have their own public Sovrin Identities on the Sovrin Ledger so they may use their Private Keys to cryptographically approve the addition of other Sovrin Trustees or Stewards.

Stewards

Stewards are trusted institutions from around the world—universities, financial institutions, healthcare providers, NGOs, governmental agencies, trust service providers, etc.—who want the benefits of Sovrin and are thus willing to commit the resources necessary to run a Node of the Sovrin Ledger. A major portion of the Sovrin Governance Framework is devoted to specifying the requirements for Stewards, including the business qualifications defined in the *Sovrin Steward Business Policies* and the technical requirements defined in the *Sovrin Steward Technical Policies* (both Controlled Documents—see Appendix A of the Sovrin Governance Framework Master Document).

Once all qualifications are met and a Steward is approved by the Sovrin Board of Trustees, the Steward must execute the Sovrin Steward Agreement with the Sovrin Foundation to establish the formal legal relationship between the two parties. The Sovrin Governance Framework (including this Glossary) is an Annex to the Sovrin Steward Agreement.

Transaction Authors

The Sovrin Ledger exists for the purpose of writing Transactions that enable the functions of the three higher layers of the Sovrin Infrastructure stack (see Appendix D). At present these include DIDs, Attributes, Schemas, Credential Definitions, Revocation Registry Definitions, and Revocation Registry Entries. A goal of the Sovrin Foundation is to enable any Sovrin Entity (Individual, Organization, Thing) that requires a public Sovrin Identity to be able to write these Transactions to the Sovrin Ledger. The Sovrin Entity acting in that role is called a **Transaction Author**.

The vast majority of Transaction Authors are likely to be Organizations because they are the ones most likely to be Issuers who need their Credentials to be publicly verifiable. By contrast, most Individuals will not need to write to the Sovrin Ledger directly because the vast majority of their DIDs will be Pairwise Pseudonymous, i.e., shared privately in the context of a specific Connection (see Appendix A and

Appendix F).

However, in some cases Individuals may also need to be Transaction Authors because they need public Sovrin Identities—either for discoverability or to issue Credentials that can be publicly verified. And the same applies to certain classes of Things, especially those that play core roles in supply chains or IoT (Internet of Things) networks.[6]

Transaction Endorsers

The right side of Figure E is labelled **Public Write Access**. This is the policy under which any Transaction Author will be able to write directly to the Sovrin Ledger without the use of any intermediary. As explained in the preamble to *Sovrin Ledger Access Policies*, Public Write Access has not been implemented yet due to regulatory uncertainties about the treatment of Personal Data. However it is a goal of the Sovrin Foundation, the Sovrin Governance Framework Working Group, and the Global Policy Working Group to clear up these uncertainties as soon as possible. Once that is done, and the necessary policies and source code have been developed and tested, Public Write Access will be implemented. This is not an easy task since it is these policies and this code that will protect the Sovrin Ledger from spam, Sybil attacks, and other malicious behavior that cannot be avoided when operating a global public utility.

In the meantime, in order to start providing value as quickly as possible, the Sovrin Governance Framework defines policies for **Permissioned Write Access**. Under these policies, a **Transaction Endorser**—a Sovrin Entity who enters a legal agreement with the Sovrin Foundation (the Transaction Endorser Agreement)—is able to authorize a Transaction by digitally signing it so it will be accepted by a Validator Node. Note that the Transaction Endorser role is only needed for Permissioned Write Access. This role will not be needed for Public Write Access.

[6] As covered in Appendix C, it is ultimately a Thing Controller who is responsible for a Thing taking an action such as posting a Transaction to the Sovrin Ledger.

Appendix F: Agent-to-Agent Protocol Layer Roles

— **Informative** —

Figure F is a visual depiction of the key business roles and interactions at the Agent-to-Agent Protocol Layer—the second layer of the four layers of Sovrin Infrastructure covered in Appendix D. This appendix will explain how these concepts and roles relate to each other.

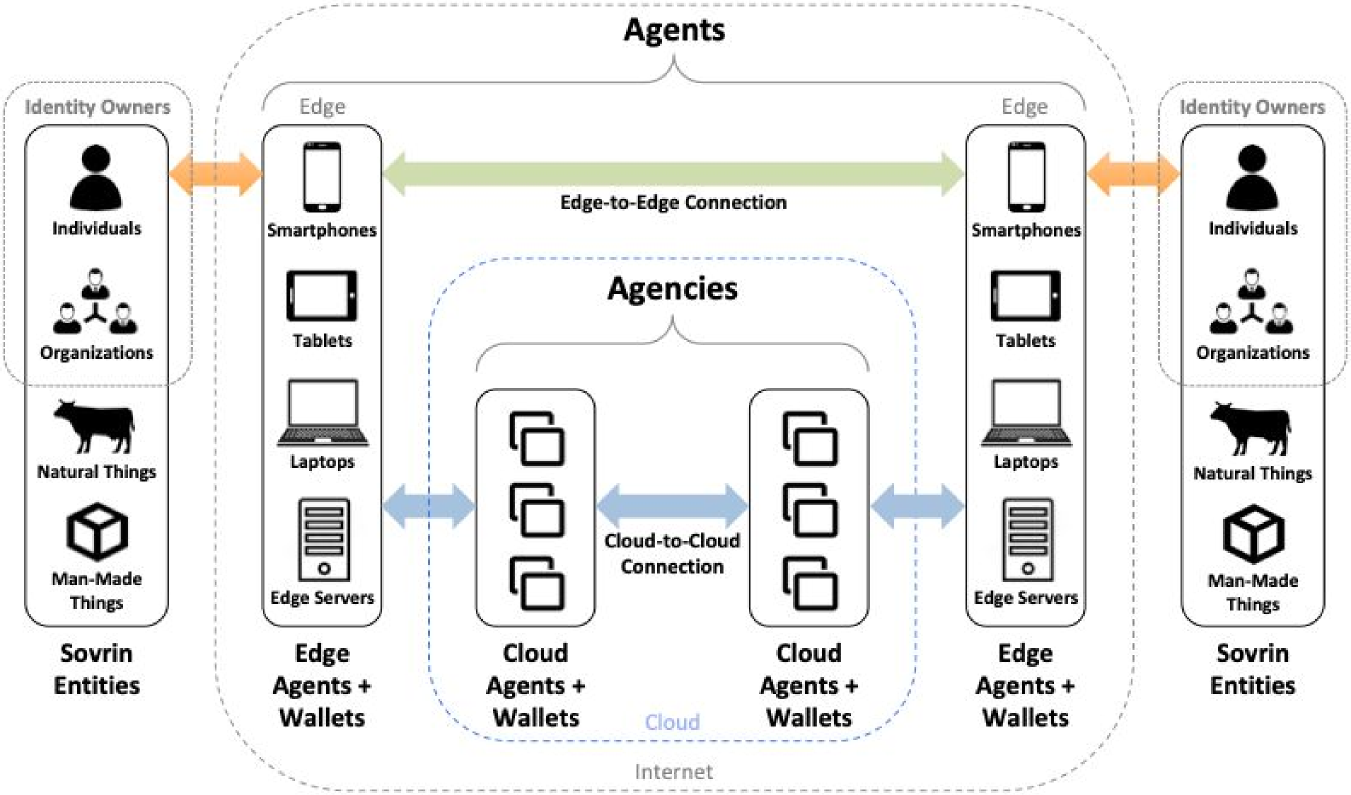

Figure F: Agent-to-Agent Layer Roles and Interactions

Agents

The concept of Agents is fundamental bedrock for Sovrin Infrastructure. The simplest way to put it is: every **Sovrin Identity is represented by an Agent and every Agent represents a Sovrin Identity**. It does not matter what kind of Sovrin Entity the Agent represents—an **Identity Owner** (Individual or Organization) or a **Thing** (Natural or Man-Made)—it always through an Agent that a

Sovrin Entity forms a Connection and shares a Sovrin Identity. This makes sense because only Agents “speak” the Agent-to-Agent Protocol and can securely read from and write to Wallets.[7]

Wallets are in fact the “other side of the coin” of Agents. The bond between the two is so strong that in Sovrin architecture, **every Wallet is associated with an Agent and every Agent is associated with a Wallet**. In fact Agents use a subset of the Agent-to-Agent Protocol called the DKMS Protocol to perform the different functions required for interoperable decentralized key management, e.g., key exchange, automated backup, offline recovery, social recovery, etc. See the DKMS Design and Architecture document for more details.

As shown in Figure F, Agents come in two fundamental types distinguished primarily by their hosting environments. **Edge Agents** operate at the edge of the Sovrin Network, i.e., either on local devices controlled directly by Identity Owners or on “edge servers” that are behind firewalls and represent trusted endpoints within an internal network. By contrast, **Cloud Agents** operate in the cloud, which is typically outside of the direct control of Identity Owners and thus subject to the terms and conditions of a cloud service provider.

The distinction between Edge and Cloud Agents is most important when it comes to key management. With Edge Agents, private keys are by definition stored “at the edge”, where in most cases they can enjoy the highest security because they are under the local control of the Identity Owner and no available via the open Internet. Cloud Agents, on the other hand, should store private keys and other cryptographic material in an HSM (Hardware Security Module) or other secure storage that is protected from unauthorized access (ideally even from the cloud service provider or hosting Agency).

Other than these distinctions, however, the job of all Agents are the same: establish and use Connections,[8] send/receive Agent-to-Agent Protocol messages, and perform actions on behalf of the Entity the Agent represents. Because these parties need to trust that their Agents are acting exclusively on their behalf, it is critical that Agencies hosting Cloud Agents—and Developers building Agent software and hardware—be fully committed to the Purpose and Principles of the Sovrin Governance Framework. (A key job of the Sovrin Trust Assurance Framework is to provide a way for this conformance to be measured and attested.)

[7] For more technical information about Agents, see this Hyperledger Indy document by Sovrin Technical Governance Board Secretary Daniel Hardman and Appendix B of the Indy Agent Architecture Reference Model (INDY-AGENT ARM) by Michael Herman.

[8] For more technical information about Connections, see this Hyperledger Indy document by Sam Curren.

Connections

Connections are covered in Appendix A. They are the fundamental unit of relationship between two Sovrin Entities—and the basis for establishing the context of any private Sovrin Identity. Figure F illustrates that in Sovrin architecture, Connections can be of two common types:

1. **Edge-to-Edge Connections** (green arrow) are where two Edge Agents communicate directly between two edge devices without using Cloud Agents or another other intermediary servers. This is required when two devices are offline, for example, if a law enforcement official needs to check a driving license in a remote area where there is no Internet.
2. **Cloud-to-Cloud Connections** (blue arrows) are where the Connection goes through one or more Cloud Agents in order to support push messaging, message queuing, group messaging, or other Agent-to-Agent Protocol features.

Agencies

While Edge Agents by definition do not require external hosting, Cloud Agents do—either self-hosting by an Identity Owner or third-party hosting by a service provider called an Agency. Sovrin Agencies are a new class of service provider comparable in many ways to ISPs (Internet service providers), email service providers, or Web service providers.

The key difference, however, is that Agencies implementing the Sovrin Governance Framework need to meet the Security by Design, Privacy by Design, and Data Protection by Design Principles of the SGF. This is a much higher bar than standard cloud hosting, and a major goal of the SGF is to incent a “race to the top” of Agency providers competing in the market to provide the strongest possible security, privacy, and data protection assurances.

Developers

Ultimately the security, privacy, and data protection capabilities of all Wallets and Agents—both Edge and Cloud—comes down to the capabilities of the software and hardware on which they are implemented. This is the role of Developers in the Sovrin ecosystem. As with Agencies, Developers must be motivated to implement code that conforms to the Sovrin Governance Framework and can be attested to under the Sovrin Trust Assurance Framework so that Identity Owners can be confident in the software and hardware they are running.

Of course Developers are also responsible for the development of the Sovrin Open Source Code that is operated by Stewards in order to run their Nodes for the Sovrin Ledger. It is vital that this community of Developers also receive adequate rewards for maintaining this vital commons resource—this is one of the goals of the *Sovrin Economic Policies*.

Appendix G: Credential Exchange Layer Roles

— Informative —

Almost all of the roles at the Credential Exchange Layer have been defined by the W3C Verifiable Claims Working Group as part of the Verifiable Credentials 1.0 specification (expected in mid-2019). These roles are illustrated in Figure G.1.

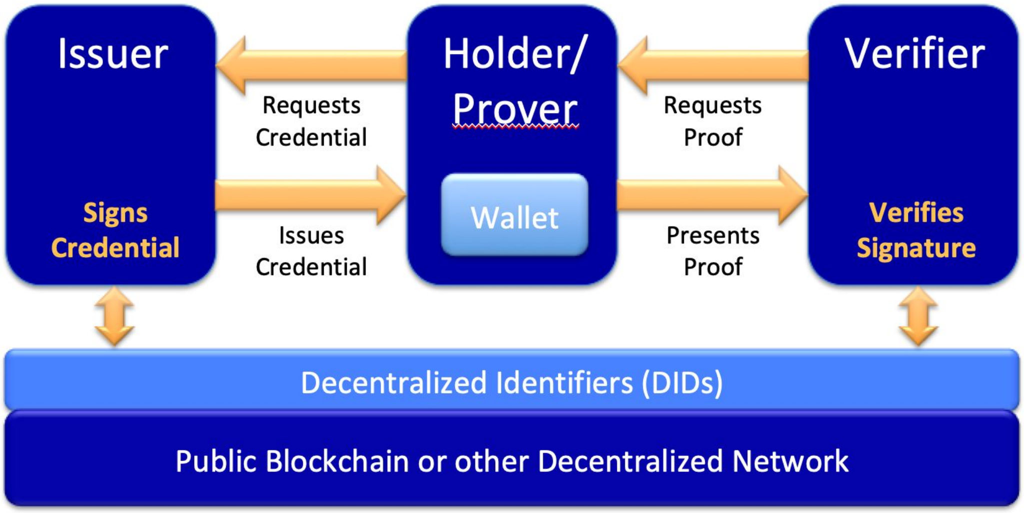

Figure G.1: Credential Exchange Layer Roles and Interactions

Subjects

Although “Subject” does not appear directly in Figure G.1, it is easy to define: it is the Entity that a DID identifies and a Credential describes. For example, the Subject of a passport or driving license is the Individual to whom it was issued. The Subject of a certificate of incorporation is the Organization to whom it was issued. The Subject of a certificate of authenticity is the Thing for which it was issued, e.g., a particular diamond, painting, or sculpture.

It is important to note that **the Subject of a Credential is not always the Holder/Prover of the Credential**. For example, while the primary Subject of a birth certificate is a baby, the actual birth certificate will typically be issued to both the mother and the father as Holders. When the child is old enough to have his/her own Wallet, another copy of the birth certificate can also be issued to the child as a Holder. Note that while the actual data on this birth certificate will be the same, the underlying cryptographic proofs will be different for each of the different Holders.

Another common example of when the Subject is not the Holder is when a Credential is issued to a Credential Registry. See Appendix H.

Issuers

Issuers are the Entities who perform the function of issuing Credentials to Holders. Every Credential has an Issuer. Most Issuers are Organizations such as government agencies (passports), financial institutions (credit cards), universities (degrees), corporations (employment credentials), NGOs (membership cards), churches (awards), etc. Almost every Organization issues credentials of some kind in its course of doing its business or pursuing its mission.

However, under SSI infrastructure, many Individuals will become Issuers, too. For example, every rating you give to a ride-share driver or home-share owner could be a credential that helps them build a portable, independent reputation. Peer-to-peer Credentials of community membership or trustworthiness are already being used to help build credit ratings for Individuals who do not have other means of gaining a credit history.

Technically, even a Thing can be an Issuer of a Credential such as digitally-signed reading from a sensor—for example a radioactivity sensor in a nuclear power plant. TPMs (Trusted Platform Modules) in computing devices can also issue Credentials attesting to the state of hardware and/or software on a device.

Holders and Provers

The Holder of a Credential is the Individual or Organization (or in some cases the Thing) to whom it was issued. The Credential is stored in the Holder's Wallet where it can be used produce Proofs. When a Holder responds to a Proof Request from a Verifier by producing a Proof, the Holder is called the Prover.

Verifiers

The Verifier is the actor that all of Sovrin infrastructure ultimately exists to satisfy. A Verifier is the Entity—typically an Organization, but it may also be an Individual or even a Thing—seeking trust assurance of some kind. Verifiers send Proof Requests to Holders seeking Proof of one or more Claims from one or more Credentials. If the Holder agrees, the Holder's Agent responds with a Proof that the Verifier must then verify to ensure that it is not fake.

Verifiers can take many forms and play many roles in different business processes. The software modules that perform verification operations may be installed in websites, cloud services, mobile apps, enterprise apps, etc. The verification process typically includes verifying that a Proof satisfies the Proof Request from the Verifier, verifying the integrity of a Proof, verifying the digital signature of the Issuer on the Proof, and verifying that the Credential has not been revoked.

Insurers

The Sovrin Governance Framework defines one more role that could play an increasingly important part in SSI infrastructure as it matures. This role—Insurer—is illustrated in Figure G.2.

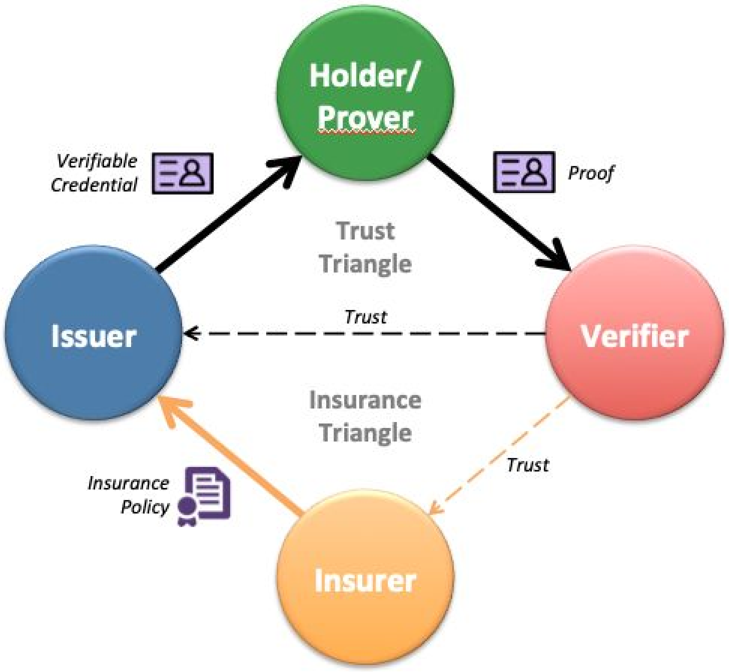

Figure G.2: The Role of an Insurer in SSI infrastructure

The "trust triangle" formed between an Issuer, Holder/Prover, and Verifier provides a way for Issuers to convey trust (in the form of a Credential) to Holders, and for Holders to convey that trust (in the form of a Proof) to a Verifier. But the higher the level of trust assurance sought by a Verifier—particularly if it is paying an Issuer for the value of a digital credential—the higher the motivation of an Issuer to mitigate the risk of an error through the purchase of insurance from an Insurer.

For more about the role of insurance in Self-Sovereign Identity infrastructure, see this article by Vinay Gupta.

Appendix H: Governance Framework Layer Roles

— Informative —

As explained in Appendix D, the purpose of the final layer of the Sovrin Stack—the Governance Framework Layer—is to fully map and integrate Sovrin solutions into the Trust Assurance requirements of the market. Figure H.1 is a conceptual diagram of the five business roles (blue boxes) the Sovrin Governance Framework defines for this layer.[9]

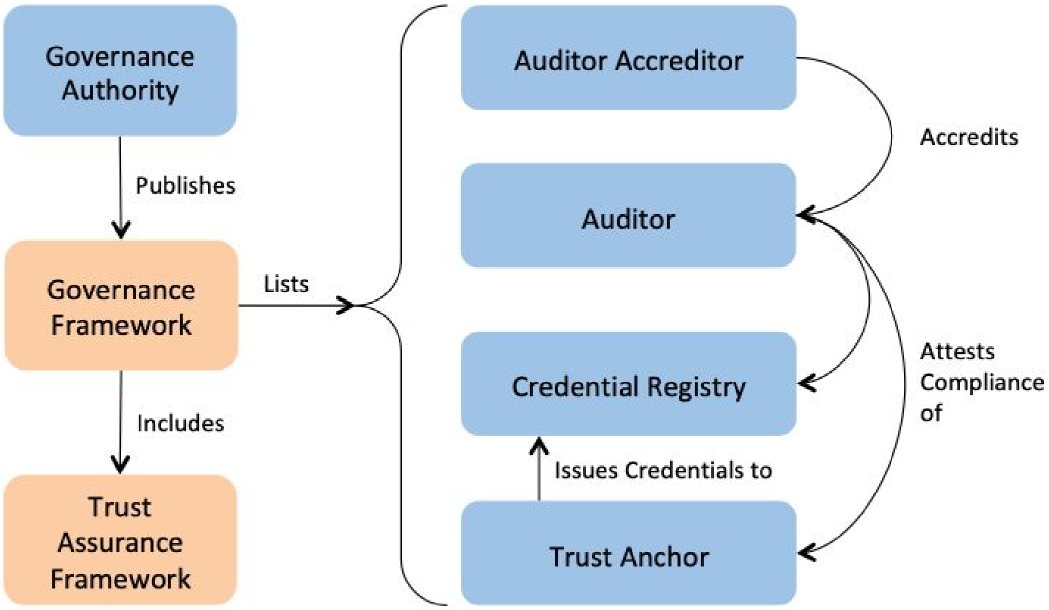

Figure H.2: Concept Diagram of the roles in the Governance Framework Layer

It is important to note that not all Trust Communities will need all roles. Each of them is optional. In fact, even a Governance Authority and Governance Framework are not strictly required. Some communities can begin to scale trust by: a) using de facto Trust Anchors, and b) implementing Credential Registries.[10] Figure H.2 illustrates the logical progression of how each of these five roles can help a Trust Community strengthen and/or scale trust.

[9] Special thanks to Scott Perry for his work on the development of this model.
[10] The Government of British Columbia's OrgBook Project has taken this approach—see more below.

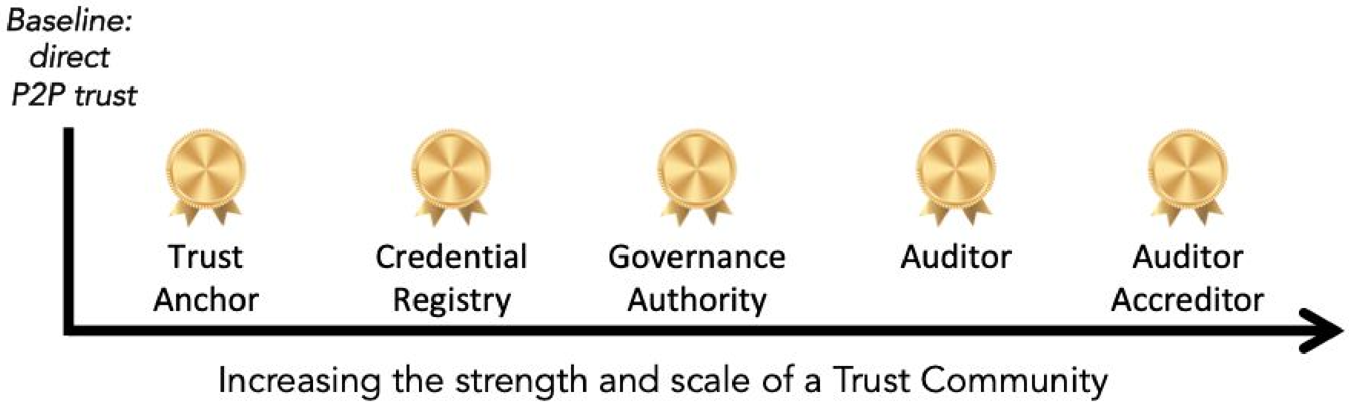
Baseline: direct P2P trust
Trust Anchor
Credential Registry
Governance Authority
Auditor
Auditor Accreditor
Increasing the strength and scale of a Trust Community

Figure H.1: Governance Framework Layer Roles

In this appendix we will explain each of these roles from left to right and show how they build on one another to strengthen and scale trust beyond the "baseline" of direct peer-to-peer trust that we all experience and use every day.

Trust Anchors

The term "trust anchor" is derived from cryptography. The Wikipedia definition is:

> In cryptographic systems with hierarchical structure, a **trust anchor** is an authoritative entity for which trust is assumed and not derived.

Relative to Sovrin Infrastructure, this means a Trust Anchor is defined in the Sovrin Glossary as:

> An Issuer who is considered by a Verifier or a Governance Authority to be authoritative for a particular set of Claims or Credentials.

In other words, when a Verifier is making a Proof Request, what the Verifier is seeking is a set of Claims that it can verify came from a Trust Anchor. A common example 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.

So establishing the Trust Anchors for a Trust Community is usually the very first step to building trust in its Credentials. As mentioned above, this step does not necessarily require establishing a Governance Authority and publishing a Governance Framework first—particularly if the natural Trust Anchors in the community are already well known. However if a Governance Framework is developed, one of its natural functions is to either: a) designate the Trust Anchors directly (using a list of Anywise DIDs), or b) specify the criteria by which Trust Anchors are Accredited and listed in a Credential Registry.

Credential Registries

Credential Registries are a new trust development mechanism that has grown out of W3C Verifiable Credentials architecture. The formal Sovrin Glossary definition of the term is:

> An Entity that serves as a Holder of Credentials issued by Trust Community Members in order to provide a cryptographically verifiable directory service to the Trust Community or to the public.

In short, a Credential Registry is **a Holder of Credentials that is not the Subject of those Credentials**. The Subject of each Credential in the registry will be some other Trust Community Member. Credentials are issued to the Credential Registry in order to provide a third-party discovery and verification function—to make it easy for Trust Community Members to see and verify who has been issued Credentials for what.

Credential Registries are most useful for Credentials containing publicly available information that avoids privacy and intellectual property issues, such as corporate registrations, business licenses, public health certificates, etc. Perhaps the best example is the OrgBook Credential Registry created using Hyperledger Indy and Sovrin by the Government of British Columbia as the start of the VON (Verifiable Organizations Network).

Credential Registries enable any set of Issuers—especially a set of Trust Anchors—to issue Credentials to a common discovery point in order to establish a baseline of publicly verifiable information about a Trust Community—even without establishment of a formal Governance Framework. This new mechanism is poised to become a powerful new tool in the evolution of the Sovrin Web of Trust.

Governance Authorities

The next step up the ladder of strengthening and scaling trust is to establish a formal Governance Authority and publish an official **Governance Framework**. This is the step the Sovrin Foundation took beginning in September 2016 with its formal incorporation—after which the Sovrin Governance Framework Working Group has been working ever since.

A Governance Authority can take any legal form appropriate for its purpose. It could be a governmental agency, a public/private partnership, a non-profit foundation, a consortium, an association, or even a conventional, for-profit corporation—whatever is best suited to engender trust in the Trust Community the Governance Authority will serve.

The primary job of the Governance Authority is to develop, publish, and maintain the Governance Framework on behalf of the stakeholders in the Trust Community. A primary purpose of the Sovrin Governance Framework is to provide a foundation for the business, legal, and technical policies required by any Governance Authority seeking to publish a Domain-Specific Governance Framework.

Auditors

Once a Governance Authority has defined a Governance Framework, the next step up the trust scaling/strengthening ladder is the inclusion of a **Trust Assurance Framework** for auditing compliance. This component of a Governance Framework specifies the criteria by which one or more Auditors can assess the conformance of Trust Anchors, Credential Registries, or other Trust Community Members (sometimes including the Governance Authority itself).

The best example is the Sovrin Trust Assurance Framework, developed as a component of the Sovrin Governance Framework V2 in order to specify compliance criteria for Sovrin Stewards and for the Sovrin Foundation itself.

Auditors are independent professionals trained in evaluating evidence provided by Trust Anchors or other Trust Community Members asserting that they are in compliance with audit criteria set forth by the Trust Assurance Framework and by independent Audit Accreditation Bodies. They issue reports attesting to their opinions which enables Governance Authorities (or their Delegates) to issue Trust Anchor Credentials and place them on Credential Registries.

Auditor Accreditors

The final step up the trust scaling ladder—one especially appropriate for Trust Communities who need to operate at global scale—is for a Governance Authority to appoint one or more Auditor Accreditors. These are professional firms who specialize in developing audit criteria out of baseline requirements in Governance Frameworks and Trust Assurance Frameworks. They evaluate applicant Auditors for their competence, independence, and quality control measures and approve them to operate under a particular Trust Assurance Framework.

Under some Governance Frameworks, Auditor Accreditors may also issue Credentials—directly to Trust Anchors and also to Credential Registries—once they receive a report from an approved Auditor.