sovrin
identity for all

v.1

Sovrin Glossary

Updated 12/20/2017

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

A

Agency. A service provider that hosts Cloud Agents and may provision Edge Agents on behalf of Sovrin Entities. Although an Agency is not required to become a Member of the Sovrin Network, if it does wish to become a Member it must: a) meet the Trust Anchor Qualifications, and b) enter into the Sovrin Agency Agreement (Appendix C).

Agent. A software program or process used by or acting on behalf of a Sovrin Entity to interact with other Agents or, via a Sovrin Client component, directly with the Sovrin Ledger. Agents are of two types: Edge Agents run at the edge of the network on a local device, while Cloud Agents run remotely on a server or cloud hosting service. Agents typically have access to a Wallet in order to perform cryptographic operations on behalf of the Sovrin Entity they represent.

Anonym. A Blinded Identifier used exactly once. See also Pseudonym and Verinym.

B

Blinded Identifier. A DID authorized to be written to the Sovrin Ledger using a Zero-Knowledge Proof in order to blind the Legal Identity of the Identity Owner. Blinded Identifiers include Anonyms and Pseudonyms. Mutually exclusive with Verinym.

Board of Trustees. The set of Trustees entrusted with governance of the Sovrin Foundation.

Business Policies. The set of policies, defined under the heading of the same name in the Sovrin Trust Framework, that specify the business rules of the Sovrin Network.

C

Claim. A digital assertion about identity attributes made by a Sovrin Entity about itself or another Sovrin Entity. The entity making the Claim is called the Issuer. The entity holding the issued Claim is called the Holder. If the Claim supports Zero Knowledge Proofs, the Holder is also called the Prover. The entity to whom a Claim is presented is called the Relying Party. A Claim may be Public Data or Private Data. Once issued, a Claim is typically stored by an Agent.

Claim Definition. A machine-readable definition of the semantic structure of a Claim. Claim Definitions facilitate interoperability of Claims and Proofs across multiple Issuers, Holders, and Relying Parties. In the future this may extend to interoperability with other trust frameworks.

Claim Offer. An invitation from an Issuer to a j to send a Claim Request to the Issuer.

Claim Request. A request to an Issuer to issue a Claim to a Holder.

Cloud Agent. An Agent that does not run at the edge of the network on a local device with which an Identity Owner interacts directly, but remotely on a server or cloud hosting service. Mutually exclusive with Edge Agent. A Cloud Agent typically has a Service Endpoint and may have access to a Cloud Wallet. Cloud agents may be hosted by an Agency.

Cloud Wallet. A Wallet that operates remotely on a server or cloud hosting service and stores its cryptographic key material securely on that server or cloud service. Cloud Wallets will typically use an HSM (Hardware Security Module). Mutually exclusive with Edge Wallet.

Connection. A digital relationship established between two Sovrin Entities via their selected Sovrin Identities to exchange Public Data or Private Data, such as Verifiable Claims, between their Agents. A Connection may or may not be published as a Claim. A Connection itself may be either Public Data or Private Data and may be formed using either a Verinym or a Pseudonym.

Connection Offer. An invitation from a one Sovrin Entity to a second Sovrin Entity to send the first Sovrin Entity a Connection Request. Connection Offers are needed only in specialized use cases; in most cases a Connection will start with a Connection Request.

Connection Request. A request from one Sovrin Entity to another Sovrin Entity to form a Connection.

D

Dependent. An Individual who needs to depend on a Guardian to administer the Individual's Sovrin Identities. Under the Sovrin Trust Framework, all Dependents have the right to become Independents. Mutually exclusive with Independent.

Developer. An Identity Owner that has legal accountability for the functionality of an Agent, or for software that interacts with an Agent or the Sovrin Ledger, to provide services to a Sovrin Entity. Although a Developer is not required to become a Member of the Sovrin Network, if it does wish to become a Member it must: a) meet the Trust Anchor Qualifications, and b) enter into the Sovrin Developer Agreement.

DDO. A DID descriptor object as defined by the DID Data Model and Generic Syntax specification. A DDO is associated with exactly one DID.

DID. A decentralized identifier as defined by the DID Data Model and Generic Syntax specification. DIDs enable interoperable decentralized self-sovereign identity management. An Identity Record is associated with exactly one DID. A DID is associated with exactly one DDO.

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

E

Edge Agent. An Agent that runs at the edge of the network on a local device, such as a smartphone, tablet, laptop, automotive computer, etc. 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 Service Endpoint, but do have access to a Edge Wallet.

Edge Wallet. A Wallet, typically used by a Edge Agent, that operates at the edge of the network on a local device and stores its cryptographic key material in a secure enclave or other secure storage on that device. Mutually exclusive with Cloud Wallet.

Entity. A resource of any kind that can be uniquely and independently identified. An Entity that obtains a Sovrin Identity becomes a Sovrin Entity.

F

Founding Steward. A Steward whose service to the Sovrin Network began by hosting a Node for the Provisional Network.

G

General Availability (GA) Network. The second stage of the Sovrin Network that begins once the Provisional Network stage ends. Once the General Availability Network stage begins, all Stewards transition from operating under the Provisional Trust Framework to operating under the General Availability Trust Framework.

General Availability (GA) Trust Framework. The second version of the Sovrin Trust Framework that will govern the Sovrin Network after the transition from the Provisional Network to the General Availability Network.

Genesis Record. The first Identity Record written to the Sovrin Ledger that describes a new Sovrin Entity. For a Steward, the Genesis Record must be written by a Trustee. For an Independent Identity Owner, the Genesis Record must be written by a Trust Anchor. For a Dependent Identity Owner, the Genesis Record must be written by a Guardian.

Guardian. An Identity Owner who administers one or more Sovrin Identities on behalf of a Dependent or a Thing. A Guardian must agree to the Guardian Obligations in the Sovrin Trust Framework.

Guardian Obligations. The set of obligations under the heading of the same name in the Sovrin Trust Framework.

H

Holder. The Sovrin Entity that has been issued a Claim by an Issuer. If the Claim supports Zero Knowledge Proofs, the Holder is also the Prover.

I

Identity Owner. A Sovrin Entity who can be held legally accountable. An Identity Owner must be either an Individual or an Organization. Mutually exclusive with Thing.

Independent. An Individual who directly controls the Private Key(s) and Master Secret(s) necessary to administer a Sovrin Identity and thus is not dependent on any other party for control. For any particular Sovrin Identity, this definition is mutually exclusive with Dependent. Note that it is possible (though not a best practice) for the same Identity Owner to be both an Independent for some Sovrin Identities and a Dependent on others.

Individual. An Identity Owner who is a natural person. Mutually exclusive with Organization.

Identity Record. A transaction on the Sovrin Ledger that describes a Sovrin Entity. Every Identity Record is associated with exactly one DID. The registration of a DID is itself an Identity Record. Identity Records may include Public Keys, Service Endpoints, Claim Definitions, Public Claims, and Proofs. Identity Records are Public Data.

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.

Issuer. The Sovrin Entity that issues a Claim for a Sovrin Identity.

Issuer Key. The special type of cryptographic key necessary for an Issuer to issue a Claim that supports Zero Knowledge Proofs.

J

Jurisdiction. A legally defined scope of authority to which an Identity Owner is bound at any one point in time. Jurisdiction is relevant to Sovrin policies to help ensure geographic diversity among Stewards and Trust Anchors. 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.

L

Legal Identity. A set of information sufficient to identify an Identity Owner for the purpose of legal accountability in at least one Jurisdiction. For the purposes of the Provisional Network, a Legal Identity may be established by reference to one or more publicly accessible Web resources such as websites, blogs, social network profiles, or other Web pages that provide sufficient information to meet this test.

Legal Policies. The set of policies, defined under the heading of the same name in the Sovrin Trust Framework, that specify the legal requirements of the Sovrin Network.

M

Master Secret. An item of Private Data used by a Prover to guarantee that a claim uniquely applies to them. The Master Secret is an input to Zero Knowledge Proofs that combine data from multiple Claims in order to prove that the Claims have a common subject (the Prover). A Master Secret should be known only to the Prover. Similar to a Private Key, but without a corresponding Public Key.

Member. An Identity Owner who enters into one or more of the Sovrin Legal Agreements with the Sovrin Foundation in order to participate in the Sovrin Network. Note that Trustees, Stewards and Trust Anchors are all Members (because they are all Identity Owners).

N

Node. A computer network server 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. All Nodes in the Sovrin Network must be operated by Stewards.

O

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

Observer Node. A Node that maintains a read-only copy of the Sovrin Ledger by communicating directly with one or more Validator Nodes. 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. A Steward may operate more than one Observer node.

Organization. An Identity Owner who is legal person of any kind except an Individual, e.g., a group, sole proprietorship, partnership, corporation, LLC, association, NGO, government, etc. Mutually exclusive with Individual.

Other Entity. An Entity identified on some other identity network external to the Sovrin Network.

P

Pairwise-Unique Identifier. A Pseudonym used in the context of only one digital relationship (Connection). See also Pseudonym and Verinym.

Privacy by Design. A set of seven foundational principles for taking privacy into account throughout the entire design and engineering of a system. Originally defined by the Information and Privacy Commissioner of Ontario, Canada. See the Wikipedia article.

Private Claim. A Claim that is sent by the Issuer to the Holder's Agent to hold (and present to Relying Parties) as Private Data but which can be verified using Public Claims and Public Data. A Private Claim will typically use a Zero Knowledge Proof, however it may also use a Transparent Proof.

Private Data. Data over which a Sovrin Entity exerts access control. Private Data should not be stored on the Sovrin Ledger even when encrypted. Mutually exclusive with Public Data.

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

Proof. Cryptographic verification of a Claim. A digital signature is a simple form of Proof. A cryptographic hash is also a form of Proof. Proofs are one of two types: Transparent or Zero Knowledge. Transparent Proofs reveal all the information in a Claim. Zero Knowledge Proofs enable selective disclosure of the information in a Claim.

Prover. The Sovrin Entity that issues a Zero Knowledge Proof from a Claim. The Prover is also the Holder of the Claim.

Provisional Network. The first stage of the life of the Sovrin Network during which Founding Stewards operate Nodes under the terms of the Provisional Trust Framework. During this stage all transactions on Sovrin Ledger will be immutable, however the volume of participants and transactions will be limited and special testing will be conducted to prepare for the transition to the second stage, called the General Availability Network.

Provisional Trust Framework. The first version of the Sovrin Trust Framework that will govern the Sovrin Network from the start of the Provisional Network until the transition to the General Availability Network.

Pseudonym. A Blinded Identifier used to maintain privacy in the context on an ongoing digital relationship (Connection). See also Anonym and Verinym.

Public Claim. A Claim that is written by an Issuer to the Sovrin Ledger in order to become Public Data. A Public Claim will typically use a Transparent Proof.

Public Data. Data over which an Identity Owner does not exert access control. All Identity Records 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 Identity Owner. 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 Identity Owner. All Public Keys published to the Sovrin Ledger are Public Data.

Public Profile. Information describing a Sovrin Service Provider, including its Legal Identity, logo(s) or other trademarks, location(s), marketing information, web links, and any other information required by the Sovrin Trust Framework to ensure full transparency about the provider's Legal Identity and qualifications.

R

Relying Party. A party who relies on a Claim or Proof in order to make a trust decision about a Sovrin Entity.

S

Self-Sovereign Identity. A general term for an identity system that provides persistent portable digital identities for Identity Owners (or for Things under the control of those Identity Owners) without requiring any centralized authorities. A Self-Sovereign Identity belongs to its Identity Owner and can never be taken away provided the Identity Owner is able to maintain control of the Identity Owner's Private Keys (or rely on a Guardian to do so).

Service Endpoint. The location of a network service, such as a Cloud Agent, operated on behalf of a Sovrin Entity.

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

Sovrin. The primary trust mark of the Sovrin Foundation held in trust on behalf of all Members.

Sovrin Agency Agreement. The contract between the Sovrin Foundation and an Agency who desires official recognition by the Sovrin Foundation. See Appendix C.

Sovrin Client. A software code module that communicates and performs cryptographic transactions with the Sovrin Ledger. Typically included as part of an Agent.

Sovrin Consensus Protocol. The Byzantine fault tolerant protocol used to communicate between Nodes to maintain the Sovrin Ledger.

Sovrin Developer Agreement. The contract between the Sovrin Foundation and a Developer who desires official recognition by the Sovrin Foundation. See Appendix D.

Sovrin Entity. An Entity that has one or more Sovrin Identities. A Sovrin Entity must be either an Identity Owner or an Thing.

Sovrin Foundation. The public trust organization chartered to govern the Sovrin Network on behalf of all Identity Owners. The Sovrin Foundation website is http://www.sovrin.org.

Sovrin Founding Steward Agreement. The contract between the Sovrin Foundation and a Founding Steward. See Appendix B.

Sovrin Identity. A set of Identity Records, Claims, and Proofs that describes a Sovrin Entity. To protect privacy: a) an Identity Owner may have more than one Sovrin Identity, and b) only the Identity Owner and the Relying Party(s) with whom a Sovrin Identity is shared knows the specific set of Identity Records, Claims, and Proofs that comprise that particular Sovrin Identity.

Sovrin Identity Owner Agreement. The contract between the Sovrin Foundation and an Identity Owner. See Appendix A.

Sovrin Ledger. The distributed, continuously-replicated global cryptographic database of Identity

Records maintained by Stewards running Nodes communicating with the Sovrin Consensus Protocol.

Sovrin Legal Agreements. The set of contracts between Members and the Sovrin Foundation as defined in the appendices of the Provisional Trust Framework or the Sovrin Trust Framework. These include the Sovrin Identity Owner Agreement, the Sovrin Founding Steward Agreement, the Sovrin Agency Agreement, and the Sovrin Developer Agreement.

Sovrin Network. The global public utility governed by the Sovrin Foundation consisting of the Sovrin Ledger, plus any supplementary ledgers and other supporting technical services as defined in the Sovrin Trust Framework.

Sovrin Open Source Code. The open source computer code base maintained by the Technical Governance Board to operate Nodes and distributed under an Open Source License. The Sovrin Open Source Code is currently maintained as the Hyperledger Indy Project at the Linux Foundation.

Sovrin Promise. The contractual obligation in the Sovrin Identity Owner Agreement for all Identity Owners to abide by the purpose, principles, and policies of the Sovrin Trust Framework.

Sovrin Service Provider. A Steward, Agency, or Developer.

Sovrin Steward Agreement. The contract between the Sovrin Foundation and a Steward. Defined in Appendix B.

Sovrin Trust Framework. The set of business, legal, and technical policies, specifications, and contracts governing the Sovrin Network. The first version of the Sovrin Trust Framework, called the Provisional Trust Framework, will govern the first stage of the Sovrin Network, called the Provisional Network. The second version, called the General Availability Trust Framework, will govern after the transition from the Provisional Network to the General Availability Network.

Sovrin Trust Graph. The graph of all Trust Anchor Connections that forms the Sovrin Web of Trust.

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

Sovrin Web of Trust. The trust model for the Sovrin Network based on Trustees, Trust Anchors and the Sovrin Trust Graph.

SSI. An acronym for Self-Sovereign Identity.

Steward. An Organization invited by the Sovrin Foundation to operate a Node. A Steward must meet the Steward Qualifications and agree to the Steward Obligations defined in the Sovrin Trust Framework. All Stewards are automatically Trust Anchors. A Steward can run either a validator or an observer node.

Steward Obligations. The set of obligations of a Steward. Defined under the heading of the same name in the Sovrin Trust Framework.

Steward Qualifications. The set of qualifications for an Organization to become a Steward. Defined

under the heading of the same name in the Sovrin Trust Framework.

T

Technical Governance Board. The set of technical experts appointed by the Board of Trustees to oversee the technical design and architecture of the Sovrin Network, the Technical Policies in the Sovrin Trust Framework, and the Sovrin Open Source Code.

Technical Policies. The set of policies, defined under the heading of the same name in the Sovrin Trust Framework, that specify the technical requirements of the Sovrin Network.

Thing. A Sovrin Entity that cannot be held legally accountable. A Thing may be an animal (e.g., pet, livestock), a natural object (e.g., house, car, phone), or a digital object (e.g., software program, network service, data structure). Mutually exclusive with Identity Owner.

Transparent Proof. A Proof that uses conventional digital signature scheme and therefore does not limit disclosure any of the information in a Claim, including the identity of the Identity Owner issuing the Proof. Mutually exclusive with Zero Knowledge Proof.

Trust Anchor. An Identity Owner who may serve as a starting point in the Sovrin Web of Trust. A Trust Anchor has two unique privileges: 1) to add new Identity Owners to the Sovrin Network, and 2) to issue Trust Anchor Invitations. A Trust Anchor must meet the Trust Anchor Qualifications and agree to the Trust Anchor Obligations defined in the Sovrin Trust Framework. All Trustees and Stewards are automatically Trust Anchors.

Trust Anchor Connection. A special type of Connection between two Trust Anchors on the Sovrin Network. See Trust Anchor Invitation.

Trust Anchor Identity. A specific DID selected by an Identity Owner to serve as the owner's exclusive Sovrin Identity in the role of Trust Anchor.

Trust Anchor Invitation. A Claim Offer from a Trust Anchor to another Identity Owner to form a Trust Anchor Connection. A Trust Anchor Invitation is an assertion that the Trust Anchor believes the Identity Owner meets the Trust Anchor Qualifications.

Trust Anchor Obligations. The set of obligations of a Trust Anchor. Defined under the heading of the same name in the Sovrin Trust Framework.

Trust Anchor Qualifications. The set of qualifications for an Identity Owner to become a Trust Anchor. Defined under the heading of the same name in the Sovrin Trust Framework.

Trustee. An Individual who is a member of the Sovrin Foundation Board of Trustees. All Trustees are automatically Trust Anchors.

V

Validator Node. A Node that validates new transactions of Identity Records and actively 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.

Verifiable Claim. A Claim that includes a Proof from the Issuer. Typically this proof is in the form of a digital signature. A Sovrin Verifiable Claim may be verified by a public key associated with the Issuer's DID.

Verinym. A DID authorized to be written to the Sovrin Ledger by a Trust Anchor so that it is directly or indirectly associated with the Legal Identity of the Identity Owner. Mutually exclusive with Anonym.

W

Wallet. A software module, and optionally an associated hardware module, for securely storing and accessing Private Keys, Master Secrets, and other sensitive cryptographic key material and optionally other Private Data used by a Sovrin Entity. A Wallet may be either an Edge Wallet or a Cloud Wallet. In Sovrin infrastructure, a Wallet implements the emerging DKMS standards for interoperable decentralized cryptographic key management.

Z

Zero Knowledge Proof. A Proof that uses special cryptography and a Master Secret to permit selective disclosure of information in a set of Claims. A Zero Knowledge Proof proves that some or all of the data in a set of Claims is true without revealing any additional information, including the identity of the Prover. Mutually exclusive with Transparent Proof.