Sovrin Glossary

A glossary of terms used in Sovrin documentation

Authored by the Sovrin Foundation

29th September 2016

sovrin.org

Sovrin Glossary

***Goal:** a single consolidated glossary for all terminology describing Sovrin infrastructure.*

Sovrin Infrastructure Providers

A single legal entity may play any combination of these roles in Sovrin infrastructure:

Steward	Operates a Sovrin ledger node (validator or observer)
Trust Anchor	Sends a request to a Sovrin validator node to register a new identity on the Sovrin ledger
Agency	A service provider that hosts Sovrin agents
Issuer	Issues claims for a Sovrin identity
Relying Party	Accepts claims from a Sovrin identity

*Note: these terms are **not capitalized** in normal usage as they are generic words. If necessary for context, prefix them with "Sovrin", e.g., Sovrin steward, Sovrin trust anchor, Sovrin agent, Sovrin issuer, etc.*

Sovrin Infrastructure Participants

Note: each of these terms must be used very precisely because they have legal implications for responsibility and liability.

Sovrin Foundation: the international non-profit organization responsible for governing the Sovrin ledger and the Sovrin identity network. Sovrin is a trademark of the Sovrin Foundation.

Identity Owner: the entity described by a Sovrin identity. May be an **individual**, an **organization** of any kind, or a **thing**. In identity systems, an identity owner is also called a *principal*. In the context of data protection regulations, an individual person acting as an identity owner is called a *data subject*. Note that a thing may not be considered legally able to "own" an identity; that ownership may be derived from the individual or organization that owns the thing.

Agent: a software process acting on behalf of an identity owner to facilitate interactions, using one or more of the identity owner's Sovrin identities. If not self-hosted, an agent is hosted by an **Agency**.

Individual: an identity owner who is a natural person.

Organization: an identity owner representing any legal or social entity except a natural person.

Thing: an identity owner that is not an individual or an organization, and thus cannot be held legally accountable.

Authority: an identity owner who is an individual or an organization, and thus can be held legally accountable.

Trustee: an individual member of the Board of Trustees that governs the Sovrin Foundation.

Trust Anchor: An **identity owner** that has permission under the **Sovrin Trust Framework** to register Sovrin identifiers and keys that enable other identity owners (individuals or organizations) to establish a **Sovrin identity**.

Network Components

Sovrin ledger ("ledger"): the distributed cryptographic database of self-sovereign identity records governed by the Sovrin Foundation. A complete copy of the ledger is maintained on both validator nodes and observer nodes.

Sovrin identity network ("Sovrin network" or "Sovrin"): the global identity network for self-sovereign identity based on the **Sovrin ledger**.

Node: a server that participates in maintaining the **Sovrin ledger**. May be a **validator node** or an **observer node**.

Client: a software application that reads records from and/or writes records to the **Sovrin ledger**.

Validator node ("validator"): a node operated by a **steward** that runs the Plenum consensus protocol to validate new identity transactions. An **identity transaction** must be submitted to and validated by a validator node in order to be written to the **Sovrin ledger**.

Observer node ("observer"): a node operated by a steward that maintains a read-only copy of the Sovrin ledger. An observer node may also push changes to subscribers.

Identities and Identity Records

Sovrin identity ("identity"): An identity owned and managed by an identity owner (a person, organization, or thing), independent of all others. Identities are multi-faceted—Alice may be known as a friend to Bob, an employee to Acme Corp, a citizen to a government, and a customer to an online retailer. From Alice's perspective, it is one identity, but only she sees it in

its totality. A Sovrin identity manifests as a collection of identifiers, key management transactions, consent receipts, and similar activity on the Sovrin Ledger. Its facets are pairwise relationships, managed in a cryptographic way by asymmetric keys, with other identity owners. An identity owner—and nobody else—can disclose information about their identity in ways that cross facet boundaries but preserve privacy.

Identity transaction ("transaction"): The act of writing a new **identity record** to the **Sovrin ledger**.

Identity record ("record"): The record written into the **Sovrin ledger** by an **identity transaction**.

Identifier record ("identifier"): An identity record that asserts an identifier for a Sovrin identity. From the standpoint of an external viewer, a Sovrin identifier record is the root of an **identity graph**.

Identifiers and Keys

Decentralized Identifier (DID): A globally unique identifier (e.g., a UUID) that has no special cryptographic properties. In Sovrin, DIDs are usually 16 bytes. DIDs must have associated **verification keys** and **signing keys** to interact securely.

Cryptographic Identifier (CID): A DID that also has cryptographic properties. In Sovrin, DIDs often act as **verification keys**, i.e., an identity owner is identified by its verification key. This saves storage space and simplifies some workflows, and it makes a DID a CID as well. The status of an identifier can change from CID to simple DID during revocation. Type-1 CIDs are established as Ed25519 verification keys. Ed25519 is the default signature scheme for Sovrin.

Nym: a shorthand term used in the Sovrin source code for a **cryptographic identifier** (CID).

Verification Key: A published asymmetric public key that's used to decrypt a message. Decryption with this key proves authenticity, because the message's sender necessarily held the corresponding signing key. Verification keys can be revoked; the current verification key for a given identifier must be looked up on the **Sovrin ledger**.

Signing Key: A never-shared asymmetric private key that an identity owner uses to encrypt messages. If this key is ever compromised, the **identity owner** can replace it with a new one.

Claims

Claim record ("claim"): an identity record that asserts one or more attributes of a Sovrin identity. A claim that asserts more than one attribute in a single identity record is called a **credential**. The origin of a claim is unambiguous, but the truthfulness of a claim must be

evaluated against the reputation of the **issuer**: a university is likely to be a reliable issuer for claims about graduation, but not for claims about the expiry of a driver's license.

Credential: a claim record that is complex in that it includes multiple claimed attributes, e.g., a driver's license that asserts a name, a birth date, an address, a permission to drive, and so forth.

Self-asserted claim: a claim record asserted by the identity owner whose identity record it describes. For example, Alice may claim that she is a fan of Manchester United, on her own authority.

Verifiable claim (aka third party claim): a claim record asserted by an identity owner other than the identity owner whose identity record it describes. The claim is verifiable in the sense that its origin may be verified by its digital signature on the Sovrin identity record.

Premium claim: a claim record for which the issuer charges a fee for a relying party to access the claim. The Sovrin Trust Framework will establish a global marketplace for premium claims. For more information see The Inevitable Rise of Self-Sovereign Identity white paper.

Receipts and Contracts

Receipt record ("receipt"): an identity record that records proof of an off-ledger transaction made by a Sovrin identity.

Consent receipt ("consent"): a receipt record that records proof that an identity owner has shared data with another party.

Link contract: A record of who is sharing data with whom, for what purpose and with what controls on its usage. As a semantic data structure, link contracts have a formal definition in the OASIS XDI Core 1.0 specification, however the general concept can be implemented in any structured data format.

Trust framework: In the context of digital identity systems, a trust framework is a combination of technical "tools" (specifications) and legal/business "rules" (policies) that enables members of a community to trust each other in online transactions. A trust framework often takes the form of a contract binding all the members of the community. See examples of various national and international trust frameworks at Open Identity Exchange (OIX).

Sovrin Trust Framework: the trust framework defined by the Trust Framework Working Group of the **Sovrin Foundation** and approved by its board of **Trustees**.

Reputation

Reputation record ("reputation"): an identity record that records a reputation event describing

a Sovrin identity. Reputation records are what form **reputation graphs**. Reputation records may be stored on-ledger or off-ledger. For more about identity and reputation, see the Open Reputation Framework paper.

Reputation trust anchor: a Sovrin identity that forms the start of a chain of reputation statements. See the Wikipedia definition (which deals mostly with PKI) and the definition in the Respect Reputation System.

Graphs

Identity graph: The graph of linked identity records that have a single identifier record as the root. For examples of identity graphs, see the OASIS XDI Core 1.0 specification.

Relationship graph: The graph of relationships between identities represented by identity graphs. Social graphs—the graph of relationships between “friends” on Facebook, “followers” on Twitter, or “connections” on LinkedIn—are all examples of relationship graphs.

Reputation graph: A specialization of relationship graphs in which each of the relationships is a reputation statement, i.e., an assertion of positive or negative reputation. For examples of a relationship graph, see the Open Reputation Framework paper.