Sovrin Frequently Asked Questions

Information from the Sovrin Foundation

Authored by the Sovrin Foundation

29th September 2016

sovrin.org

Sovrin FAQ

Note: this document is best read in combination with:

The Inevitable Rise of Self-Sovereign Identity
The Technical Foundations of Sovrin
The Sovrin Glossary

All of which can be found on sovrin.org/docs/.

What is Sovrin?

Sovrin is a global, decentralized identity network. It delivers the Internet's missing identity layer. Sovrin allows people and organisations to create portable, self-sovereign digital identities which they control, and which can't be taken away by any government or organisation. It uses a public permissioned ledger which is governed by the Sovrin Foundation.

Sovrin uses open-source distributed ledger technology. These ledgers are a type of cryptographic database that is provided cooperatively by a global pool of participants instead of a single giant database with a central administrator. In Sovrin, identity records live redundantly in many places, and accrues in transactions orchestrated by many machines. It is protected by strong, industry-standard cryptography and best practices in key management and cybersecurity. The result is a reliable, public source of truth under no single entity's control, robust to system failure, resilient to hacking, and highly immune to subversion by hostile entities.

Who governs Sovrin?

The Sovrin network is governed by the not-for-profit Sovrin Foundation. The Sovrin Foundation coordinates the stable, trusted operation of the Sovrin network. Sovrin is established at launch as a US-based 501-C3 non-profit organisation.

The Sovrin Foundation provides the "permissioned" aspect of Sovrin - the Foundation determines and manages the terms of reference, the Technology Governance Board, the approval of new Stewards, and the management of existing Stewards along with the overall health of the network.

How does Sovrin work?

The Sovrin network is a global group of interconnected nodes. When mature, the network will be run by numerous public and private sector organisations around the world, according to the rules laid down by the Sovrin Foundation. The nodes run an extension of the redundant byzantine fault tolerant consensus protocol to ensure that the ledger which keeps

records of all identity transactions is reliable, complete and immutable. Nodes are run by stewards. Stewards are approved into the network by the Sovrin Foundation.

What is “Self-Sovereign” Identity?

Self-sovereign identity is an identity which the identity owner (an individual or organisation) owns and controls. No organisation, government or other individual can take this identity away from the identity owner. In the digital world, it is the natural evolution of online identity mechanisms. Self-sovereign identity means security, control and portability. For the first time, people can create a truly portable digital identity which they can use anywhere with full control and consent recording, and which isn’t reliant on any single organisation or provider.

How do people create a Sovrin identity?

Usually, individuals or organisations are ”bootstrapped” onto Sovrin by a trust anchor, such as a bank, identity provider or other organisation with whom they already have a trusted relationship. Individuals can initiate their own Sovrin identity if they wish. Once an initial Sovrin identity record has been established, an identity owner can add additional identity “claims” (attributes, identity transactions, identity proofs) to their Sovrin identity. Only the identity owner can see and manage this data. As Sovrin matures, more and more organisations will provide the ability to write verified claims to people's’ Sovrin identities as they recognise the value of the network and the ability to rely on the data written by other claims issuers.

How are Sovrin identities used?

When a Sovrin identity owner wants to use their identity, they will be asked for some information by a relying party; examples might include name, address and date of birth. The identity owner will find those entries in their Sovrin identity which match the requirements of the relying party, and then give the relying party access to those records. The relying party will be able to, with the identity owner’s permission, verify the issuer of the identity data which the issuer will have digitally signed. When data is shared in this way, a consent record is written to the identity owner’s and relying party’s Sovrin identity records to confirm that the data has been shared, by whom, to whom, for what reason, and with what constraints.

Is Sovrin an Identity Provider?

Sovrin is not an identity provider (IDP). It is a global identity network which allows people to securely store identity information over which the individual has total control. This is called “self-sovereign” identity. We envisage that it will be used by IDPs and many other services at the request of individuals who need to prove their identity and user many other related services. Think of Sovrin as a global, secure layer for storage of identity transactions.

How does Sovrin work with Identity Providers?

Sovrin will enable IDPs and others to, at the identity owner's request, utilise verifiable data from authoritative providers to carry out high assurance ID proofing checks. It does not include the capacity for face to face checks but can record that these have been carried out. It is envisaged that IDPs will be able to carry out identity proofing at a far lower cost than currently possible. IDPs and others who create complex, composite and value-added identity information will be able to write these to an identity owner's Sovrin identity record, and if they so desire, set a price for other organisations to use this data - these are called "Premium Claims".

Who benefits from Sovrin?

Identity owners will get a fully portable digital identity which they control and which nobody can take away from them. Identity providers and other similar services will get a full open method for securely accessing identity owners' data, with their permission, and with consent recorded. Information providers ("claims issuers") get a way to digitally provide identity owners with verified identity data which the identity owner can store and manage securely. Organisations get an organisational identity, and can use advanced reputation ratings to create the successor to net promoter scores.

Where does the source code come from?

Evernym have developed the source code for Sovrin. The open-source software, called Plenum, that nodes use to run the ledger is hosted on Github.

What's in it for Evernym?

Evernym developed the technology behind Sovrin. Evernym has gifted this to the Sovrin Foundation, recognising that an independent governance framework is necessary to fulfil Sovrin's potential.

Evernym is building products and services which utilise Sovrin. Evernym will provide these products and services to organisations, who want to use Sovrin but don't want to build their own, for a fee. Evernym also has competitors building on Sovrin. It is an open ecosystem, and identities are portable.

How can I rely on the Sovrin identity data supplied from another organisation?

Sovrin itself does not dictate any trust rules beyond validating that a Sovrin identity record is: a) validly formatted, b) digitally signed by a submitter that has write permission. All decisions about trust in a Sovrin identity record depend on trust relationships between the parties reading and writing the records (e.g., if my mother says I'm a pilot, that's not as good as the FAA saying I'm a pilot). Each relying party will be able to verify the issuer of a claim, e.g., doctor's association, driving license issuer, bank, insurance company, etc. and also that the claim has not changed since writing. So each relying party can determine if the claim issuer is one they can trust.

In many cases point-to-point trust is not efficient enough; this is where trust frameworks fit. A community of relying parties (e.g., banks, insurance companies, universities, government agencies) can define a trust framework that will define the rules for verifying a claim or credential to a certain level of assurance (LOA), and then issuers operating under that trust framework can indicate the LOA that applies when they write a claim to the ledger.

Who is liable for a bad actor misbehaving?

There are many scenarios of misbehaviour so this area could justify its own workshop. Here are a few examples:

The easiest approach is to compare it to what happens today with paper claims, but with a much stronger digital verification capability. Today I can present a photocopy of my birth certificate countersigned by “a responsible person like a solicitor or doctor”. With Sovrin I can present a digital version of my birth certificate, which can be verified immediately as having been written by the General Registry Office and to be unchanged since it was written. I can also present any number of other claims (assuming the issuers have written then to my ID chain on Sovrin). The relying party will determine the validity of those claims for their purposes.

Should a node operator misbehave, their behavior can be detected by the underlying consensus algorithm and their changes rejected. Further, they can be ejected by the Sovrin foundation (e.g. for attempting to alter the ledger after the fact).

How are credentials revoked?

Every claim (credentials/attributes) can be revoked by the issuer. The form revocation takes depends on the type of credential and privacy requirements. Revocation does not necessarily mean deletion. If I passed my driving test and am entitled to drive, the DVLA can write a record to my Sovrin chain attesting to this. Should I lose my licence, my name, address & date of birth still remain valid, but my entitlement to drive has been removed. It can be reinstated later. Sovrin enables issuing organisations to trigger revocation on claims that they have issued.

What data standards does Sovrin Use?

Data standards define the rules under which data are represented within a system or in the case of Sovrin, between systems. Take the recording of a date as an example. For some, month, day, year is the format, for others, day, month, year is the convention. Data standards formalise these conventions. An ontology is the common language that machines use to understand and interpret the data standards in order to properly exchange information. XDI dictionaries represent the ontology technology within the Sovrin Identity Network. XDI dictionaries enable clear definition of attributes for people, organisations and things.

What is the user economic model? Can a user set a price for access to their data?

Sovrin has the concept of Premium Claims, which will be implemented in a future release. Premium Claims are priced by the Issuer. The issuer may be an organisation or an individual. If the user self-issues a Premium Claim (e.g. I am a vegan and live in Guildford and want to buy a BMW), he/she could set a price for it and the market will determine if it is a price worth paying. In addition, individuals may receive a slice of payments for premium claims about them which they choose to reveal to relying parties.We anticipate that 3rd party service providers will create innovative services that create new markets for personal data—to the benefit of both individuals and organisations.

What happens if a key is compromised?

A key revocation is recorded on the ledger. The revoked key is superseded by an updated value, and no subsequent misuse is possible. (The details of revocation are beyond the scope of this FAQ, but are documented elsewhere.)

What data is stored on the Sovrin ledger?

Sovrin is dedicated to self-sovereign identity. It allows you to store information on the ledger or point to it off the ledger. At a very basic level it holds identities, keys and transaction proofs and pointers.

The decision as to whether to hold data on- or off-ledger may be based on multiple factors, including: how long the data needs to be available and the level of confidence in the longevity of the issuer (or the location where the data is stored), and the level of sensitivity of the data.

Can the Sovrin ledger be forked?

While the Sovrin ledger runs on open source code that could be forked by anybody at any time, the actual operational Sovrin ledger is maintained by the Sovrin Stewards and governed by the Sovrin Foundation. The Foundation controls whether the Sovrin ledger is ever forked; nobody can independently fork it. If it were ever necessary to fork the Sovrin ledger, it would only be because the Foundation determined it was in the best interests of users.

What are the incentives/benefits for operators of Sovrin nodes (“Stewards”).

Node operators (stewards) are not expected to make a profit running a node; however, there are both hard and soft benefits.

1. Hard benefits:
    a. Direct access to Sovrin reduces latency for reading and writing.
    b. Once mature, costs can be covered via a slice of revenue from the Sovrin Foundation as a result of the premium claims market (see below).
2. Soft benefits:

a. Every Sovrin steward builds a positive reputation by operating a Sovrin node that meets the security, privacy, availability, and reliability standards laid down by the Sovrin Foundation. This will earn it significant kudos.
b. Being a Sovrin steward is a highly distinguished role within the Sovrin network.