Sovrin Provisional Trust Framework

Sovrin Board of Trustees

22nd March 2017

Sovrin.org

Sovrin Provisional Trust Framework

This document was produced by the Sovrin Trust Framework Working Group and approved by the Sovrin Foundation Board of Trustees on 22 March 2017 to become the operational trust framework for the Sovrin Provisional Network.

Sovrin Trust Framework Working Group: Drummond Reed (Chair), Scott Blackmer (Counsel), John Best, Luca Boldrin, Tim Brown, Shaun Conway, Mawaki Chango, Rick Cranston, Scott David, Steve Fulling, Nathan George, Darrell O'Donnell, Nichola Hickman, Adam Lake, Jason Law, Antti Jogi Poikola, Markus Sabadello, Peter Simpson, Andy Tobin, Eric Welton, and Phil Windley.

1. Introduction

The purpose of the Sovrin Trust Framework is to define the business, legal, and technical terms under which all Members of the Sovrin Network agree to cooperate. To do this, the Sovrin Trust Framework is divided into the following sections:

Section #	Name
1	Introduction
2	Purpose and Principles
3	Terminology and Definitions
4	General Obligations of the Sovrin Foundation
5	Business Policies
6	Legal Policies
7	Technical Policies
8	Technical Specifications
9	Versioning and Amendments

In addition, the Sovrin Trust Framework specifies the following legal contracts between the Sovrin Foundation and Members:

Appendix	Name
A	Sovrin Identity Owner Agreement
B	Sovrin Steward Agreement
C	Sovrin Agency Agreement
D	Sovrin Developer Agreement

For a general introduction to Sovrin, please see the Sovrin Library page of the Sovrin website.

2. Purpose and Principles

The purpose of the Sovrin Network is **to provide a global public utility for decentralized identity** that adheres to the principles below.

2.1. Independence and Self-Sovereignty

An Identity Owner shall have the right to completely and permanently own and control one or more Sovrin Identities without the need to rely on any external administrative authority and without the fear that a Sovrin Identity will ever be taken away.

2.2. Guardianship

An Identity Owner who does not have the capability to directly control the owner's Sovrin Identities (a Dependent) shall have the right to appoint another Identity Owner who has that capability (an Independent) to serve as the owner's Guardian. A Dependent has the right to become an Independent by claiming full control of the Dependent's Sovrin Identities. A Guardian has the obligation to promptly assist in this process provided the Dependent can demonstrate that the Dependent has necessary means to exert control.

2.3. Diffuse Trust

The process and policies for selecting Stewards and Trust Anchors shall not concentrate power in any single Individual, Organization, Jurisdiction, Industry Sector, or other special interest. Diffuse Trust shall take into account all forms of diversity among the Identity Owners that the Sovrin Network serves.

2.4. Web of Trust

The process and policies for selecting Stewards and Trust Anchors shall not be hierarchical but enable interlocking peer-to-peer trust networks that form an overall Sovrin Web of Trust.

2.5. System Diversity

The process and policies for selecting Stewards shall maximize diversity of hosting locations, environments, networks, and systems in order to optimize availability and security.

2.6. Interoperability

The design, governance, and operation of the Sovrin Network shall endeavor to provide Members with maximum interoperability of their Sovrin Identities, Public Data, and Private Data both within the network and with other external systems and networks.

2.7. Security

The design, governance, and operation of the Sovrin Network shall provide Members with security for their Sovrin Identities and Private Data to the greatest extent feasible consistent with the other principles herein.

2.8. Privacy

The design, governance, and operation of the Sovrin Network shall provide Members with privacy for their Sovrin Identities and Private Data to the greatest extent feasible consistent with the other principles herein.

2.9. Portability

The design, governance, and operation of the Sovrin Network shall provide Members with portability of their Public Data and Private Data to the greatest extent feasible consistent with the other principles herein.

2.10. Accountability

Members of the Sovrin Network shall be accountable to each other for conformance to the purpose, principles and policies of the Sovrin Trust Framework.

2.11. Transparency

The Sovrin Foundation and the Sovrin Network shall operate with full transparency to the greatest extent feasible consistent with the principles herein, including the proceedings of the Sovrin Board of Trustees and the Technical Governance Board, the development and

distribution of Sovrin Open Source Code, the qualification and operation of Stewards, and the listing of Agencies and Developers.

2.12. Accessibility, Inclusion, and Non-Discrimination

The Sovrin Foundation and the Sovrin Network shall be accessible to all Identity Owners without discrimination and with accommodation for physical, economic, or other limitations of Identity Owners to the greatest extent feasible.

2.13. Collective Best Interest

The Sovrin Foundation shall govern the Sovrin Network in the collective best interests of all Identity Owners and shall not favor the interests of any single Identity Owner or group of Identity Owners over the interests of the Members as a whole.

3. Terminology and Definitions

The subjects of digital identity, security, privacy, and trust can be extremely difficult to describe without well-defined terminology. This section first introduces the primary terms used in the Sovrin Trust Framework and then provides an alphabetical glossary of all defined terms (which will always appear in First Letter Capitals).

3.1. Formatting Conventions

All defined terms in the Sovrin Trust Framework appear in First Letter Capitals.

In policy definitions, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" appearing in all capital letters are to be interpreted as described in RFC 2119.

Text in magenta is special instructions or policies that exist only in the Sovrin Provisional Trust Framework. In some cases these are policies that are planned to take effect in the Sovrin Trust Framework V1 that will govern the General Availability Network.

3.2. Legal Taxonomy of Sovrin Entities and Identities

Figure 1 helps explain the relationship, from a legal standpoint, between the different types of entities and identities defined in the Sovrin Trust Framework.

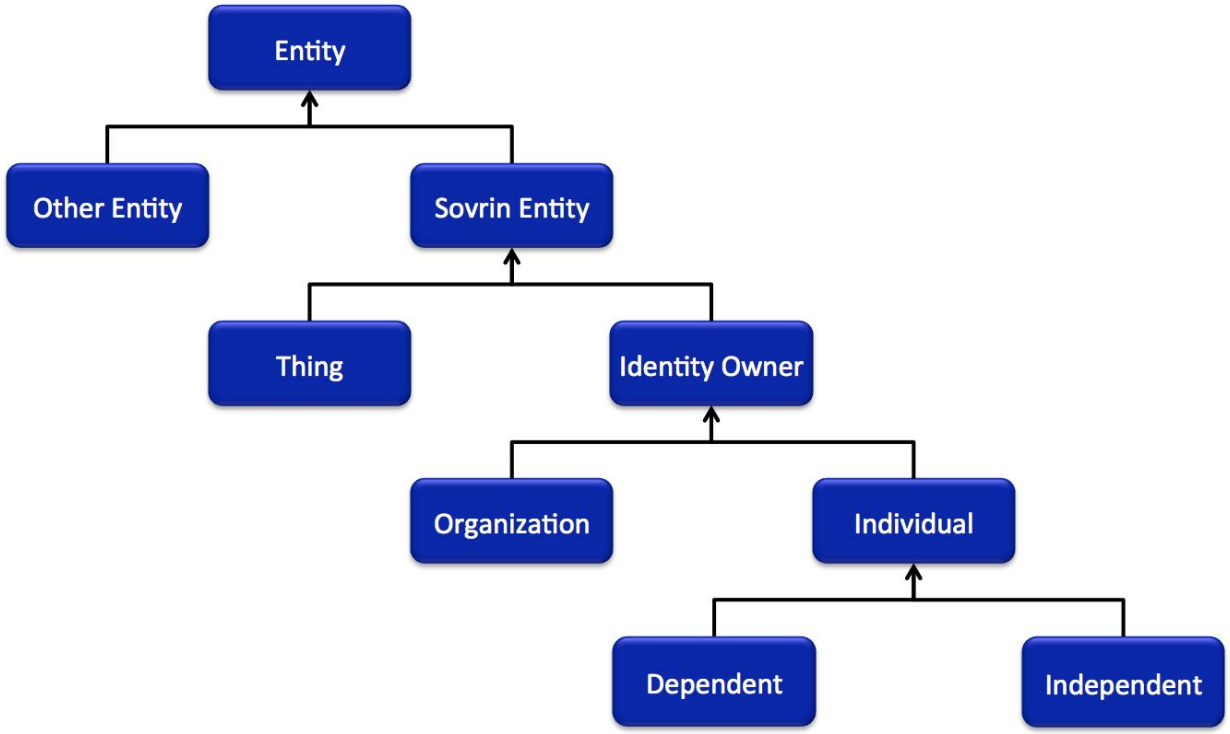

Figure 1: Taxonomy of Sovrin entity and identity types from a legal standpoint

1. An **Entity** is any independently identifiable resource of any kind. It is a **Sovrin Entity** if it has at least one Sovrin Identity on the Sovrin Network; otherwise it is an **Other Entity** identified on some other identity network. (Note that an Other Entity may become a Sovrin Entity simply by obtaining a Sovrin Identity.)
2. Sovrin Entities are divided into two types: **Identity Owners**, who may be held legally accountable for their actions on the Sovrin Network, and **Things**, which cannot be held legally accountable for their actions (accountability for Things falls to the Identity Owners responsible for them).[1] Things may be animals (e.g., pets, livestock, game), physical objects (e.g., cars, buildings, computers, phones), and digital objects (e.g., files, photos, apps, databases).
3. Identity Owners are one of two types: **Individuals** (natural persons) or **Organizations** (legal persons of any form, such as corporations, partnerships, LLCs, NGOs, governments, etc.). While both can be held legally responsible for their actions, only Individuals take such actions directly in the real world. Organizations are abstract entities whose actions are always taken indirectly by Individuals acting on their behalf.
4. At any one point in time, Individuals fall into one of two categories: **Independents**, who have direct control of the Private Keys needed to administer a Sovrin Identity, or **Dependents**, who are not in a position to directly control their Private Keys, either because of legal or physical incapability (such as a child or elderly parent), economic or

[1] The Sovrin Trust Framework is not by itself an identity assurance framework, however it may interoperate with other identity assurance frameworks such as those based on NIST 800-63 or eIDAS.

political incapability (such as a refugee), or computing or networking incapability (such as not having a device or online access).

The distinction between Independents and Dependents is particularly important because control of an owner's Private Keys is what makes an Identity Owner truly self-sovereign. Even though a Dependent is still an Identity Owner with the right to control the owner's Sovrin Identities, the Dependent must depend on another Identity Owner, called a **Guardian**, to control the Private Keys and do the actual administration. The Sovrin Trust Framework contractually defines the rights and obligations of Dependents and Guardians to each other in order to facilitate this important new type of digital trust relationship.

3.3. Sovrin Entities, Sovrin Identities, DIDs, and Identity Records

Figure 2 explains core components of Sovrin's privacy architecture.

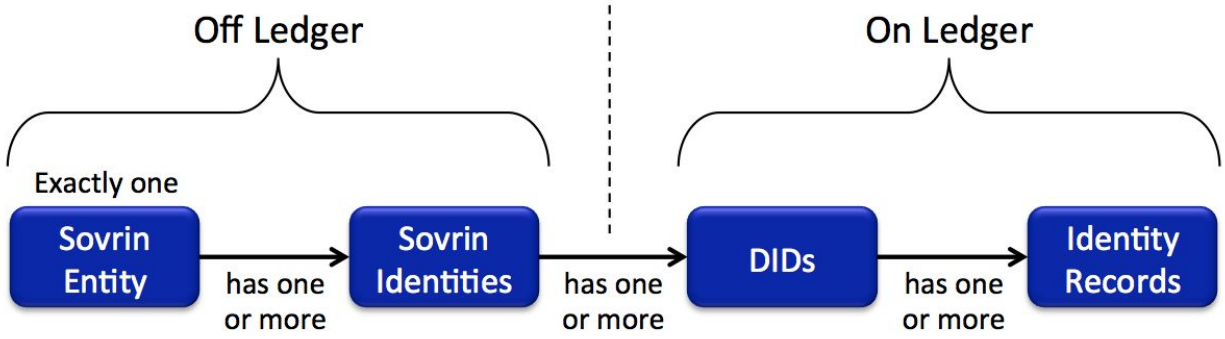

Figure 2: Fundamental components of Sovrin's privacy architecture

1. **Each Sovrin Entity is unique**, i.e., exactly one Individual, Organization, or Thing capable of having a Sovrin Identity.
2. **Every Sovrin Entity has at least one Sovrin Identity**—*but it is not limited to having only one*. Individuals, for example, may have as many Sovrin Identities as they need to protect their privacy and keep contextual separation in their lives (e.g., home, school, work, hobbies). A contextually separate identity is often called a *persona*.
3. **Every Sovrin Identity has one or more DIDs** (decentralized identifiers)—globally unique identifiers that do not require any centralized registration authority and serve as indexing values on the Sovrin Ledger. See the DID specification. Note that while each Sovrin DID is a part of at least one Sovrin Identity, a Sovrin Identity may be composed of Identity Records from more than one DID.
4. **Every DID has one or more Identity Records**. These are the actual data records on the Sovrin Ledger that contain information about the Sovrin Entity they describe, e.g., Public Keys, Service Endpoints, Public Claims, Proofs, etc.

Here is how these core components contribute to Sovrin privacy architecture:

1. **A Sovrin Identity is never fully defined on the Sovrin Ledger.** While each DID

represents at least a component of a Sovrin Identity, only the Identity Owner knows the "map" of which DIDs and Identity Records (on-ledger) and Claims and Proofs (off-ledger) that have been shared with which Relying Parties to compose a complete Sovrin Identity. So the ultimate definition of a Sovrin Identity always remains the Identity Owner's Private Data.

2. **DIDs and Identity Records should not reveal any Private Data.** All Private Data should be stored off-ledger, behind Service Endpoints controlled by the Identity Owner, and only shared via a secure peer-to-peer connection between Sovrin Agents or Apps. Only Public Data should appear on the Sovrin Ledger.
3. **Off-ledger Claims and Proofs can be verified via on-ledger Public Data.** With standard public/private key cryptography, an Identity Record containing a Public Key may be used to verify a Proof signed with a Private Key. However, with Zero Knowledge Proof cryptography, Identity Owners may prove Claims about themselves (e.g., "I am over 18", or "I have a bank account", "I am a citizen of X country") without revealing their identity or the underlying data behind the proof (i.e., birthday, bank account number, national ID number).

3.4. Anonyms, Pseudonyms and Verinyms

Figure 3 illustrates how Sovrin privacy architecture supports the full spectrum of identity, i.e., identifiers that range from highly anonymous to highly verifiable.

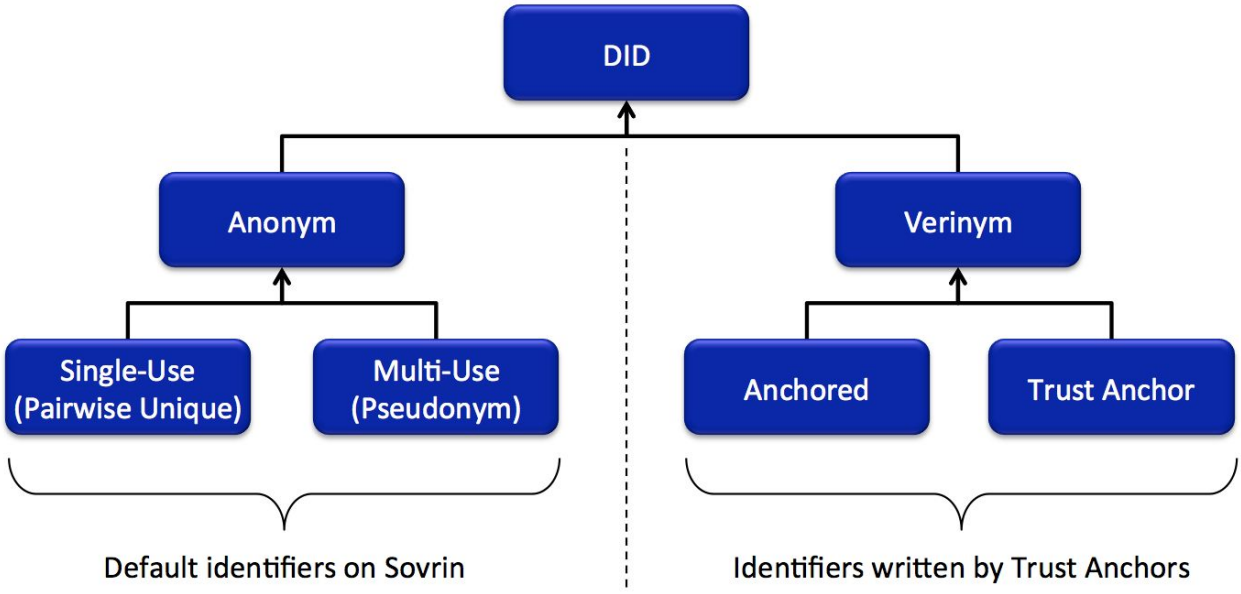

Figure 3: Sovrin identifiers support the full spectrum of identity from anonymity to verinymity

1. **Anonyms** are DIDs that are authorized to be written to the Sovrin Ledger using a Zero-Knowledge Proof so they are blinded as to the Legal Identity of the authorizing Identity Owner. Anonyms maximize privacy. Anonyms on Sovrin are one of two types:
    a. **Single-Use Anonyms**—also known as **Pairwise-Unique Identifiers**—are used

by the Identity Owner only for only a single digital relationship (potentially even just for a single interaction).
    b. **Multi-Use Anonyms** are used by the Identity Owner for more than one digital relationship—a concept better known as **Pseudonyms**.
2. **Verinyms** are DIDs that are authorized to be written to the Sovrin Ledger using the digital signature of a Trust Anchor so that they may be directly or indirectly associated with the Legal Identity of the Identity Owner. Verinyms are needed for the legal accountability of Trust Anchors. Verinyms on Sovrin are one of two types:
    a. A **Trust Anchor Verinym** is the DID of a Trust Anchor itself. This DID is required to have at least one Public Claim asserting the Trust Anchor's Legal Identity. See the next section for more about Trust Anchors.
    b. An **Anchored Verinym** is the DID for an Identity Owner for whom the Trust Anchor can confirm consent to the Sovrin Identity Owner Agreement (Appendix A).

As a global public utility for decentralized identity, it is critical to Sovrin Privacy by Design architecture to establish that Anonyms are the default identifier for all Sovrin Entities. If the design of the Sovrin Network incented Identity Owners to use Verinyms instead of Anonyms, Anonyms might become "second class identifiers" to the detriment of privacy. To avoid this, the goal of the Sovrin Technical Governance Board is to make Anonyms and Verinyms as functionally similar as possible. This preserves Anonyms as the default behavior, makes Privacy by Design the default choice, and means correlation, when needed, may be provided intentionally using Zero Knowledge Proofs. The only strong justification for using Verinyms is Trust Anchors as described in the next section.

3.5. Trustees, Trust Anchors, and the Sovrin Web of Trust

As a public permissioned ledger, the Sovrin Network is both an identity network and a *trust network*—a way for Identity Owners to establish a basic level of trust between their Sovrin Identities. This section explains the special roles that Trustees and Trust Anchors play in building the Sovrin Web of Trust.

1. **Trustees** are Individuals who serve as members of the Sovrin Foundation Board of Trustees. Together with the Sovrin Foundation as an Organization, they are the starting point for the Sovrin Web of Trust, as they approve the initial Stewards and Trust Anchors.
2. **Trust Anchors** are Individuals or Organizations for whom there is sufficient public evidence of their trustworthiness and accountability to believe they will live up to the **Sovrin Promise**—the contractually-binding obligation of all Identity Owners to abide by the purpose, principles, and policies of the Sovrin Trust Framework.

The **Sovrin Web of Trust** is formed as Trust Anchors form **Connections** with other Sovrin Identity Owners. A Connection is a digital relationship between two Sovrin Identity Owners that can be cryptographically verified using their Trust Anchor Identities. If a Trust Anchor believes

another Identity Owner is qualified to be a Trust Anchor, the Trust Anchor may issue a **Trust Anchor Invitation**. An Identity Owner who accepts a Trust Anchor Invitation (which requires agreeing to the **Trust Anchor Obligations**) now has a **Trust Anchor Connection** and becomes a Trust Anchor. This is how the Sovrin Web of Trust can grow organically without any centralized control.

Due to the diffuse nature of trust networks, it is expected that the vast majority of Sovrin Identity Owners will eventually become Trust Anchors. From the standpoint of the Sovrin Trust Framework, the primary purpose of this Sovrin Web of Trust is to protect the Sovrin Network itself. However, the ability of the Sovrin Network to share cryptographically verifiable Sovrin Identities, Claims, and Proofs means the Sovrin Web of Trust may also serve as a foundation for other trust networks.

3.6. Sovrin Infrastructure Provider Roles

Sovrin infrastructure is maintained by three types of providers. Note that a single Organization may play all three roles.

1. **Stewards** are Organizations who operate the Nodes of the Sovrin Ledger. The initial Stewards are appointed by the Sovrin Foundation Board of Trustees—this is what makes Sovrin a *public permissioned ledger*. Stewards must enter into the Sovrin Steward Agreement with the Sovrin Foundation (Appendix B).
2. **Agencies** are Organizations who host Agents on behalf of Identity Owners. Only Agencies who wish to be officially recognized by the Sovrin Foundation need to enter into the Sovrin Agency Agreement with the Sovrin Foundation (Appendix C).
3. **Developers** are Organizations or Individuals who develop Apps that use the Sovrin Network. Only Developers who wish to be officially recognized by the Sovrin Foundation need to enter into the Sovrin Developer Agreement with the Sovrin Foundation (Appendix D).

3.7. Definitions

All capitalized terms in the Sovrin Trust Framework (except those defined inline) are defined in this section. Also, each of the Principles stated in section 2 are also defined terms.

Agency. A service provider that hosts Agents on behalf of Identity Owners. To become a Member of the Sovrin Network, an Agency must: a) meet the Trust Anchor Qualifications, and b) enter into the Sovrin Agency Agreement (Appendix C).

Agent. A software program or process acting on behalf of a Sovrin Entity to facilitate interactions with other Agents or the Sovrin Ledger. If not self-hosted, an Agent is hosted by an Agency. An Agent may or may not have a publicly accessible Service Endpoint and may or may not store Public Keys, Private Keys, Public Data, or Private Data.

Anonym. 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. An Anonym used only in the context of a single digital relationship (Connection) is a Pairwise-Unique Identifier; an Anonym used in the context of more than digital relationship is a Pseudonym. Mutually exclusive with Verinym.

App. A software program created by a Developer and used by an Identity Owner to interact with the Identity Owner's Agent(s) or the Sovrin Ledger. One typical (but not required) function of an App is to store the Identity Owner's Private Keys and Master Secrets.

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.

Claim. A digital assertion 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.

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 Holder to send a Claim Request to the Issuer.

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

Client. A software program or component that generates, stores and/or accesses Public Keys and Private Keys to perform transactions with the Sovrin Ledger. A Client may be a component of an App or a component of an Agent.

Connection. A digital relationship established between two Sovrin Entities via their selected Sovrin Identities to exchange Public Data or Private Data between their Apps and/or 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 an Anonym or a Verinym.

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.

Dependent. An Individual who must 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 App. To become a Member of the Sovrin Network, a Developer 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. An Identity Record is associated with exactly one DID. A DID is associated with exactly one DDO.

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

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

General Availability Network. The second stage of the Sovrin Network that begins when 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 Sovrin Trust Framework.

Genesis Record. The first Identity Record written to the Sovrin Ledger to describe a new Sovrin Entity. 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. 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.

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.

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, 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.

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

Jurisdiction. A legally defined scope of authority to which an Identity Owner is bound. 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.

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.

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.

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 must be operated by Stewards.

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.

Pairwise-Unique Identifier. An Anonym used 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 or App 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 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 Sovrin Network during which Founding Stewards operate Nodes under the terms of the Provisional Trust Framework.

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. An Anonym which is used in the context of more than one digital relationship (Connection). See also 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 elliptic curve cryptography, a public key is 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.

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

Service Endpoint. The location of a network service, such as an 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 of the Sovrin Network.

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

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. Includes 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/or 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.

Sovrin Promise. The contractual obligation of all Members 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 version of the Sovrin Network, called the Provisional 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.

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.

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.

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 either an animal (e.g., pet, livestock), a natural object (e.g., house, car, phone), or digital object (e.g., software program, network service, data structure). Mutually exclusive with Identity Owner.

Transparent Proof. A Proof that uses conventional cryptography and therefore does not limit disclosure any of the information in a Claim, including the identity of the Prover. 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.

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.

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.

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

4. General Obligations of the Sovrin Foundation

The Sovrin Foundation shall have the obligation to:

1. Develop and maintain the Sovrin Trust Framework, including the Provisional Trust Framework and any subsequent revisions, to govern the operation of the Sovrin Network in accordance with the purpose and principles in Section 2.
2. Appoint and oversee the Technical Governance Board responsible for the development and maintenance of the Sovrin Open Source Code and the Technical Policies of the Sovrin Trust Framework in accordance with the purpose and principles in Section 2.
3. Develop and maintain Sovrin Trust Marks as specified by the policies and procedures herein.
4. Invite Stewards as specified by the policies and procedures herein.
5. Invite Trust Anchors as specified by the policies and procedures herein.
6. Accept Agencies who voluntarily become Members of the Sovrin Network.
7. Accept Developers who voluntarily become Members of the Sovrin Network.
8. Monitor and analyze the performance and reliability of the Sovrin Network and when necessary enforce Sovrin Trust Framework policies to ensure its continued health.
9. Promptly notify Stewards of:
    a. Suspected attacks, malware or other threats that could reasonably affect Stewards' operations or equipment.
    b. Sanctions or changes in status affecting particular Identity Owners, Agencies, Developers, or other Stewards.
    c. Material changes in relevant software, technical standards, or other policies required to operate a Sovrin Node or interact with the Sovrin Ledger.
10. Conduct public education and promotion of the Sovrin Network and its purpose,

principles, policies, and uses.

11. Ensure the economic sustainability of the Sovrin Foundation and the Sovrin Network so as to be able to carry out these obligations on behalf of all Members.

5. Business Policies

5.1. Identity Owner Obligations

Identity Owner Obligations are specified in the Sovrin Identity Owner Agreement. See Appendix A.

5.2. Steward Qualifications

1. A Steward MUST comply with all Legal Policies applying to a Steward.
2. A Steward MUST comply with all Technical Policies applying to a Steward prior to going live on the Sovrin Network and to maintain compliance thereafter.
3. A Steward MUST be willing and able to contribute the technical resources necessary to operate a Node at the service levels specified in the Technical Policies.
4. A Steward MUST comply with all Trust Anchor Qualifications prior to going live on the Sovrin Network.
5. For the General Availability Network, a Steward MUST belong to one of the following categories:
    a. An official governmental agency of a UN-recognized nation.
    b. A governmentally regulated institution (e.g., credit union, bank, healthcare provider, insurance company, etc.) with at least 5 years operating history.
    c. A non-governmental organization (NGO) with at least 10 years operating history.
    d. An accredited university with at least 10 years operating history.
    e. A certificate authority (CA) with at least 10 years operating history.
    f. A Sovrin Service Provider with a demonstrable record of serving the Sovrin community.
    g. A commercial organization willing to make a clear and strong documented public commitment, including a financial commitment, to supporting the mission of the Sovrin Foundation.
6. For the General Availability Network, a Steward candidate MUST submit a written application to the Executive Director of the Sovrin Foundation or his/her designee self-attesting to the candidate's qualifications according to the criteria above and explaining the candidate's motivations to become a Sovrin Steward.

5.3. Steward Invitations

1. The Sovrin Foundation MUST invite only Organizations meeting the Steward Qualifications to become a Steward.
2. For the Provisional Network, the Sovrin Foundation's Steward invitation process:
    a. SHOULD follow the principle of System Diversity.
    b. SHOULD follow the principle of Diffuse Trust.
    c. SHOULD give priority to qualified Organizations who volunteer to make the commitment to serve as a Founding Steward.
    d. SHOULD give priority to Social Purpose Organizations.
3. For the General Availability Network, once there is a sufficient number of Stewards, the Sovrin Trust Framework SHOULD incorporate policies for ensuring System Diversity and Diffuse Trust that can be enforced algorithmically and dynamically by the Sovrin Open Source Code operating on all Nodes to determine which Nodes should be operating as Validator Nodes at any one point in time.

5.4. Steward Disqualification and Remediation

1. For the Provisional Network, a Steward who no longer complies with the Steward Qualifications SHOULD be suspended until such time as the Steward is able to provide reasonable assurance to the Sovrin Foundation that: a) the Steward is back in compliance, and b) the Steward will be able to maintain compliance for the foreseeable future.
2. For the General Availability Network, this policy MUST be extended to enumerate the specific stages and notice periods required for both suspension and remediation.

5.5. Steward Obligations

Steward Obligations are specified in the Sovrin Founding Steward Agreement. See Appendix B.

5.6. Trust Anchor Qualifications

1. For the Provisional Network, to serve as a Trust Anchor, an Identity Owner MUST:
    a. Establish exactly one Trust Anchor Identity.
    b. Publish at least one publicly available Verifiable Claim associating the Identity Owner's Trust Anchor Identity with the Identity Owner's Legal Identity.
    c. Receive at least one Trust Anchor Invitation to form a Trust Anchor Connection with another Trust Anchor or the Sovrin Foundation.
    d. Accept that Trust Anchor Invitation and in doing so agree to the Trust Anchor Obligations.
2. For the General Availability Network, the Board of Trustees SHOULD adjust the threshold number of Trust Anchor Connections required to qualify as a Trust Anchor so as to ensure the integrity of the Sovrin Web of Trust.

5.7. Trust Anchor Invitations

1. The Sovrin Foundation MUST invite only Identity Owners meeting the Trust Anchor Qualifications to become a Trust Anchor.
2. For the Provisional Network, the Sovrin Foundation's Trust Anchor invitation process:
    a. SHOULD follow the principle of Diffuse Trust.
    b. SHOULD give priority to qualified Trust Anchors who have contributed directly to the Sovrin community.
    c. SHOULD give priority to qualified Social Purpose Organizations or their contributors.
3. For the General Availability Network, these policies SHOULD be extended following the principle of Diffuse Trust to enable all qualified Identity Owners to receive Trust Anchor Invitations.

5.8. Trust Anchor Disqualification and Remediation

1. For the Provisional Network, a Trust Anchor who no longer complies with the Trust Anchor Qualifications MUST be suspended until such time as the Trust Anchor is back in compliance.
2. For the General Availability Network, this policy MUST be extended to enumerate the specific stages and notice periods required for both suspension and remediation.

5.9. Trust Anchor Obligations

1. A Trust Anchor MUST maintain exactly one Trust Anchor Identity.
2. A Trust Anchor MUST maintain a current valid publicly available Verifiable Claim associating their Trust Anchor Identity with their Legal Identity.
3. When adding a new Identity Owner to the Sovrin Network, a Trust Anchor MUST ensure that the Identity Owner has agreed to the Sovrin Identity Owner Agreement.
4. When issuing a Trust Anchor Invitation to an Identity Owner, a Trust Anchor MUST:
    a. Verify that the Identity Owner's Trust Anchor Identity has a Verifiable Claim to the Identity Owner's Legal Identity.
    b. Verify that the Identity Owner agrees to the Trust Anchor Obligations.
    c. Have no knowledge that the Identity Owner is in violation of the Sovrin Identity Owner Agreement or these Trust Anchor Obligations.

5.10. Guardian Obligations

1. With regard to a Dependent and the Dependent's Sovrin Identities, a Guardian MUST agree to act in the capacity of an information fiduciary as described in https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.
2. A Guardian MUST promptly act on the instructions of a Dependent to transfer guardianship to another Guardian.
3. A Guardian MUST act promptly on the instructions of a Dependent to become an Independent provided that the Dependent can demonstrate the means by which the

Dependent will claim control over the Dependent's Sovrin Identities, including providing the Guardian with the Public Key required to control each Sovrin Identity to be claimed.

5.11. Code of Conduct

Policies in this section will be defined in the Sovrin Trust Framework V1.

6. Legal Policies

The Sovrin Legal Agreements, to which the Provisional Trust Framework is an annex, are contracts between Members and the Sovrin Foundation that will be interpreted within the framework of existing law. The policies in this section set forth requirements for the Sovrin Legal Agreements. For additional context on international legal issues relating to identity management and trust services, the following resources are recommended:

- The background documents submitted for the UNCITRAL Colloquium on Identity Management and Trust Services, including submissions from:
    - Austria, Belgium, France, Italy, and Poland
    - The Identity Management Legal Task Force of the American Bar Association
    - The Russian Federation
- The EU eIDAS regulations

6.1. Identity Owners

1. An Identity Owner MUST be an Individual or an Organization.
2. An Identity Owner MUST agree to the Sovrin Identity Owner Agreement (Appendix A).

6.2. Stewards

1. A Steward MUST be an Organization legally registered in at least one Jurisdiction.
2. A Steward MUST comply with the laws and regulations of the Jurisdiction(s) in which the Steward is legally licensed to operate.
3. For the Provisional Network, a Founding Steward MUST agree to the Sovrin Founding Steward Agreement (Appendix B).
4. For the General Availability Network, a Steward MUST agree to the Sovrin Steward Agreement.

6.3. Agencies

Policies in this section will be defined in the Sovrin Trust Framework V1.

6.4. Developers

Policies in this section will be defined in the Sovrin Trust Framework V1.

6.5. Sovrin Trust Mark

1. For the Provisional Network, the Sovrin Foundation MUST grant Stewards a license to use the Sovrin Trust Mark "Sovrin Founding Steward".
2. For the Provisional Network, the Sovrin Foundation MUST grant Trust Anchors a license to use the Sovrin Trust Mark "Sovrin Trust Anchor".

6.6. Dispute Resolution

1. For the Provisional Network, disputes MUST be resolved via arbitration managed by the International Chamber of Commerce.
2. For the General Availability Network, the Sovrin Trust Framework SHOULD include a dispute resolution policy for all Members that is as equitable and efficient as possible, for example, ICC Arbitration Rules, with arbitration in New York under New York law unless otherwise agreed by the parties.

7. Technical Policies

7.1. Steward Nodes

For the Provisional Network, a Node operated by a Founding Steward:

1. MUST run as a Validator Node (Observer Nodes will not be introduced until the General Availability Network).
2. MUST run the current release of the Sovrin Open Source Code as designated by the Technical Governance Board.
3. MUST upgrade to a new version of the Sovrin Open Source Code within 3 business days of notification of the new release by the secretary of the Technical Governance Board.
4. MUST register all Node configuration data required by the Pool Ledger.
5. MUST run a server operating system that receives timely patches from its vendor or community.
    a. For Linux, the base OS is less than 2.5 years old.
    b. For Windows, the base OS is less than 4 years old.
6. MUST run on server-class hardware that is less than 4 years old.
7. If a Node is run on a VM, the Steward:
    a. MUST run on a mainstream hypervisor that receives timely patches from its vendor or community.
    b. SHOULD apply hypervisor patches on a regular basis.

8. MUST run in a machine that is dedicated to the validator, i.e., a single-purpose (physical or virtual) machine that does not provide services unrelated to Sovrin.
9. MUST have at least one IT-qualified person assigned to administer the node, and at least one other person that has adequate access and training to administer the box in an emergency.
10. MUST supply contact info for all administrators to the Sovrin Foundation, whose accuracy is tested at least quarterly (e.g., by sending an email and/or text that doesn't bounce).
11. SHOULD have high-speed (e.g., 100Mbit or gigabit) access to the internet--preferably with highly available, redundant pipes.
12. SHOULD have at least one dedicated NIC for Sovrin Validator Node consensus traffic, and a different NIC to process external requests.
13. MUST have a stable, static, world-routable IP address.
14. SHOULD maintain a system backup or snapshot or image such that recovering the system from failure could be performed in an hour or less.
15. MUST be a single machine, NOT a cluster. (High availability in Sovrin is achieved via the consensus algorithm; hot-swapped machines in a cluster configuration may actually make the network less reliable.)
16. SHOULD have 2 or more cores.
17. MUST have at least 8 GB of RAM and an ample amount (e.g., 1-2 TB) of reliable (e.g., RAIDed) disk space.
18. MUST run NTP and maintain a system clock that is demonstrably in sync within two seconds.
19. SHOULD run in a locked datacenter with at least one layer of keycard access to provide an audit trail. (We recommend SSAE 16 type II compliance, but other standards may also be acceptable.)
20. SHOULD be able to weather modest power brownouts and blackouts (up to 60 minutes).
21. SHOULD be isolated from internal systems of a Steward (since the Validator Node is publicly visible and thus an inappropriate candidate for access to privileged internal networks).
22. SHOULD apply the latest security patches with latency of 1 week or less (24 hours or less is recommended).
23. MUST run a firewall that disallows public ingress except on ports used by the Validator Node software (different machines may choose to expose ledger features on different ports, so no standard port setup is required). Ssh, Remote Desktop, and similar remote access tools may be enabled, however ingress for these tools must be constrained in some way that excludes the public but allows access for admins.
24. SHOULD allow remote access (including over SSH) only with two-factor authentication.
25. MUST NOT allow access (remote or local) by anyone other than assigned admins.

7.2. Steward Security Monitoring and Reporting

For the Provisional Network:

1. Stewards MUST run a weekly report using the oscap tool and SCAP policies approved by the Sovrin Foundation's Technical Governance Board, and email the results to its administrators and to the Sovrin Technical Governance Board. The email to the Sovrin Technical Governance board MAY have a latency of up to a week to give an admin time to react to issues before the Technical Governance Board sees a report and publishes data derived from it.
2. If a Steward detects a compromise of its Node, it MUST notify the Technical Governance Board in writing ideally within 1 hour, but at least within 24 hours, and work closely with the Technical Governance Board and/or its designed representative to troubleshoot.
3. If the Technical Governance Board detects compromise of a Node, it MUST notify the relevant Steward in writing ideally within 1 hour, but at least within 24 hours, and work closely with the Steward to troubleshoot.

7.3. Sovrin Ledger Write Permissions

For the Provisional Network, the following policies specify which Sovrin Entities have permission to write to the Sovrin Ledger under what conditions:

1. Trustees MAY write:
    a. Genesis Records for themselves.
    b. Genesis Records for new Trustees, Technical Governance Board members, Stewards, or Trust Anchors as permitted by a majority vote of the Board of Trustees.
2. Stewards MAY write:
    a. Genesis Records for new Trust Anchors.
3. Trust Anchors MAY write:
    a. Genesis Records for new Independent Identity Owners except Trustees or Stewards.
    b. Trust Anchor Invitations for new Trust Anchors.
4. Guardians MAY write:
    a. Identity Records for Dependent Identity Owners.
5. Identity Owners MAY write:
    a. Identity Records for themselves.

7.4. Sovrin Ledger Transaction Limitations

During the Provisional Network, the following policies specify the limitations on write transactions to the Sovrin Ledger:

1. All DIDs MUST be Verinyms until the Provisional Trust Framework is revised to include policies governing the provisioning of Anonyms.
2. Identity Owners MUST NOT update a DDO more than three times in one twenty-four hour period.

3. A DDO MUST NOT exceed 100K in size.

7.5. Agencies

Policies in this section will be defined in the Sovrin Trust Framework V1.

7.6. Developers

Policies in this section will be defined in the Sovrin Trust Framework V1.

8. Technical Specifications

For the Provisional Network, the Sovrin Trust Framework relies on the following technical specifications.

1. DID Data Model and Generic Syntax 1.0
2. Sovrin DID Method Specification

9. Versioning and Amendments

1. The Provisional Trust Framework MAY be revised during the Provisional Network stage upon approval by a majority vote of the Board of Trustees.
2. Any new version of the Provisional Trust Framework MUST be published to the Sovrin Foundation website once it is approved.
3. The Provisional Trust Framework MUST be replaced by the Sovrin Trust Framework V1 as approved by the Board of Trustees prior to the transition from the Provisional Network to the General Availability Network. The Sovrin Trust Framework V1 MUST incorporate the long-term rules for versioning and amendments.

10. Appendix A: Sovrin Identity Owner Agreement

See this link.

11. Appendix B: Sovrin Founding Steward Agreement

See this link.

12. Appendix C: Sovrin Agency Agreement

Will be added in the Sovrin Trust Framework V1.

13. Appendix D: Sovrin Developer Agreement

Will be added in the Sovrin Trust Framework V1.