Sovrin Trust Framework V2

STAKEHOLDER REVIEW DRAFT 01

2018-09-07

Sovrin Board of Trustees

Sovrin.org

STATUS NOTE

This is a living document maintained by the Sovrin Trust Framework (STF) Working Group. This is NOT the latest version approved by the Sovrin Foundation Board of Trustees. Rather it is a "live" draft of the Sovrin Trust Framework V2 (STF2) open for comments and input from the Sovrin community. Note that the comments and revisions in this draft are **proposals only** and have not yet been approved by the Sovrin Board of Trustees.

To see the latest version approved by the Trustees in PDF format, see the links below.

- Prior version with comments. This document has live edits and comments. The edits have been carried over to this document but the comments will be manually dealt with as a group.
- Sovrin Provisional Trust Framework 2017-06-28 ⇐ LATEST APPROVED VERSION
- Sovrin Provisional Trust Framework 2017-03-22

NOTE: NEW STRUCTURE

The organization of V2 represents a new structure as explained in the Introduction section below. Under this new structure, this document serves as Annex 1 of the revised Sovrin Steward Agreement. Annex 2 is the standalone Sovrin Glossary.

TK is used throughout to denote places where content is "to come".

PREAMBLE

This document was produced by the Sovrin Trust Framework Working Group. The latest version was approved on__________________ by the Sovrin Foundation Board of Trustees to become the operational trust framework for the Sovrin Network and the foundation for other Domain-Specific Trust Frameworks.

Sovrin Trust Framework Working Group: Drummond Reed (Chair), Scott Blackmer, John Best, Luca Boldrin, Mike Brown, Tim Brown, Shaun Conway, Mawaki Chango, Rick Cranston, Scott David, Oskar van Deventer, Steve Fulling, Nathan George, Dan Gisolfi, Nicky Hickman, Riley Hughes, Adam Lake, Jason Law, Darrell O'Donnell (STF Coordinator), Adewale Omoniyi, Scott Perry, Antti Jogi Poikola, Elizabeth Renieris, Markus Sabadello, Joyce Searls, Peter Simpson, Ryan Sulkin (Counsel), Andy Tobin, Eric Welton, and Phil Windley

Note: All terms in First Letter Capitals are defined in the Sovrin Glossary.

INTRODUCTION

The Sovrin Trust Framework (STF) serves as the constitution for the Sovrin Network as well as a foundation upon which Domain-Specific Trust Frameworks (DSTFs) can be built. DSTFs allow many different Trust Communities to create specialized trust frameworks that leverage the STF to address their specific needs, e.g.:

- Government / Jurisdictional Bodies (e.g. countries, provinces, states, cities, sectors, consortia, distributed organisations)
- Accreditation Bodies (e.g. Colleges of Medicine; Legal Societies; Professional Associations)
- Formal Organizations and Affiliations (e.g. Non-Government Organizations; Trade Organizations; Credit Unions)
- Educational Institutions (e.g. universities and colleges)

Regardless of the domain, the STF and the Sovrin Web of Trust Model it defines provides a standard set of principles, policies, terminology, and standards that can be used by any DSTF.

Note that the Sovrin Foundation and its Trust Framework Working Group also define one DSTF, the *Sovrin Directory Trust Framework*, as explained below. The relationship of all the documents comprising the Sovrin Trust Framework V2 (STF V2) family is shown in Figure 2.

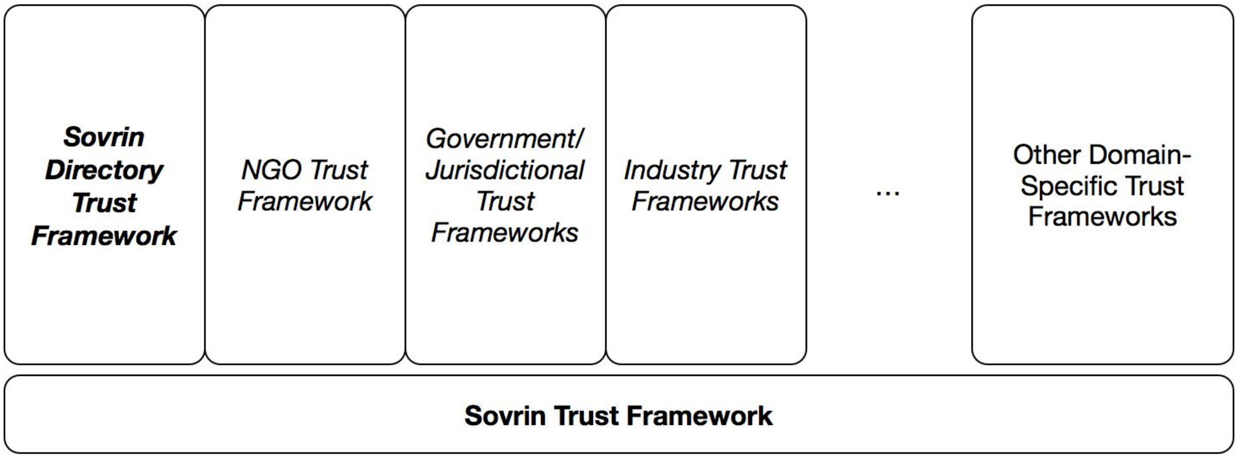
Sovrin Directory Trust Framework
NGO Trust Framework
Government/ Jurisdictional Trust Frameworks
Industry Trust Frameworks
...
Other Domain-Specific Trust Frameworks
Sovrin Trust Framework

Figure 1: *Sovrin Trust Framework provides a foundation for Domain-Specific Trust Frameworks.*

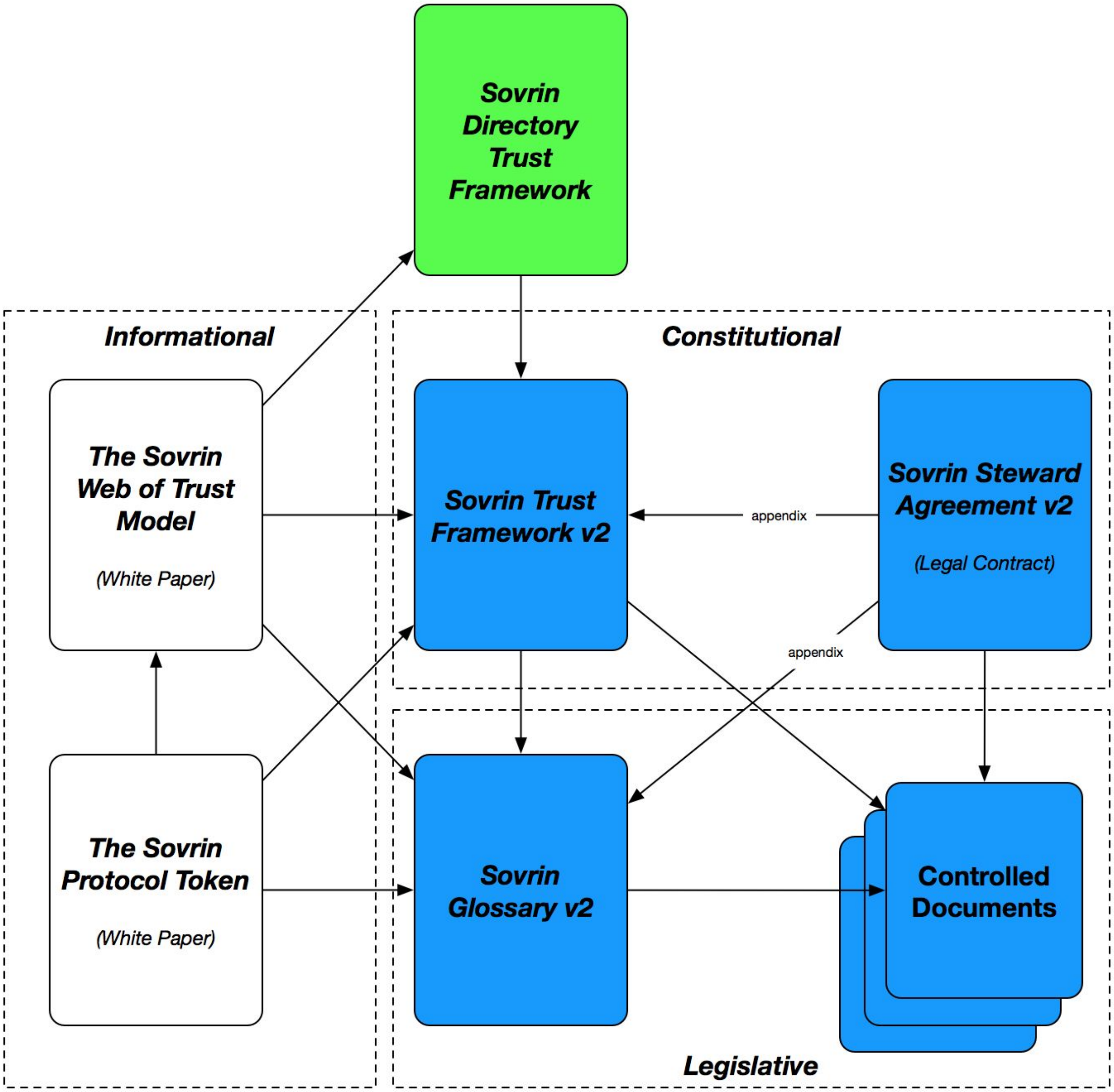
Sovrin Directory Trust Framework
Informational
Constitutional
The Sovrin Web of Trust Model
(White Paper)
Sovrin Trust Framework v2
appendix
Sovrin Steward Agreement v2
(Legal Contract)
appendix
The Sovrin Protocol Token
(White Paper)
Sovrin Glossary v2
Controlled Documents
Legislative

***Figure 2**: Documents in the Sovrin Trust Framework V2 family*
(Blue = Normative, Green = DSTF, White = Informative)

The normative documents in the STF V2 are:

- **Sovrin Trust Framework V2**—the present document.
- **Sovrin Glossary V2**—the terminology and definitions that apply across Sovrin broadly.
- **Sovrin Steward Agreement V2**—the legal contract between Sovrin Stewards and the Sovrin Foundation.
- **Controlled Documents** —technical specifications, standards, policies, etc., that are independently maintained and versioned either by the Sovrin Foundation (e.g., the

Sovrin Crisis Management Plan) or by external standards bodies (e.g., W3C, OASIS).

Although it is not normatively part of the STF V2, the **Sovrin Directory Trust Framework** (SDTF) is being produced in parallel with the STF V2 to provide a standard mechanism for navigating the Sovrin Web of Trust.

In addition to the normative documents, the Sovrin Foundation is also producing two white papers to provide further information about the STF V2:

- **The Sovrin Web of Trust Model** is an overall guide to the STF V2. It explains the key concepts underlying the decentralized web of trust architecture that is the mission of the Sovrin Foundation. It also explains the role of each of the documents in the STF V2 family, and provides a guide to reviewing them as a whole.
- **The Sovrin Protocol Token** is a white paper devoted specifically to explaining the role and function of the Sovrin Token in the Sovrin Network.

1 PURPOSE

The purpose of the Sovrin Ledger is to provide a decentralized global public utility for self-sovereign identity that serves as the foundation for the Sovrin Network.

The purpose of the Sovrin Network is to enable the Sovrin Web of Trust—a decentralized global web of trust interconnecting all Identity Owners and the Things they control.

The purpose of the Sovrin Trust Framework (STF) is to define the business, legal, and technical terms for the Sovrin Web of Trust, thereby providing a foundational layer upon which Domain-Specific Trust Frameworks (DSTF) can be built.

The purpose of the Sovrin Foundation is to provide decentralized governance for the Sovrin Ledger, Sovrin Network, and Sovrin Trust Framework on behalf of all Identity Owners.

2 CORE PRINCIPLES

The following principles guide the development of policies in the STF and all DSTF that inherit them.

2.1 Self-Sovereignty

Identity Owners shall have the right to completely and permanently own and control one or more Sovrin Identities without reliance upon any external administrative authority.

1. An Identity Owner alone shall determine what Sovrin Identity Data describe its Sovrin Identities.
2. An Identity Owner alone shall determine how and for what purpose its Sovrin Identity Data is processed.
3. An Identity Owner alone shall determine who has access to its Sovrin Identity Data and to which Relying Party the Identity Owner will share its Identity Data.
4. An Identity Owner's Sovrin Identity Data shall be portable as determined by the Identity Owner.
5. An Identity Owner alone shall have the right to Delegate control of these functions.

2.2 Guardianship

An Individual who does not have the capability or the desire to directly control the owner's Sovrin Identity Data (a Dependent) shall have the right to appoint another Identity Owner who has that capability (an Independent or an Organization) 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 Identity Data. 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. Guardianship shall not be confused with Delegation. Guardianship under the Sovrin Trust Framework may be mapped to various legal constructs, including power of attorney, conservatorship, and _____________.

2.3 Openness and Interoperability

The Sovrin Network shall use open standards and avoid mechanisms that would prevent Identity Owners from having interoperability or portability of their Sovrin Identity Data both within the Sovrin Network and with other external networks and systems.

2.4 Accountability

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

2.5 Sustainability

The Sovrin Network shall be designed and operated to be both economically and environmentally sustainable for the long term.

2.6 Transparency

The Sovrin Foundation and the Stewards in their Sovrin Ledger Roles shall operate with full openness and transparency to the greatest extent feasible consistent with the principles herein, including the proceedings of the Sovrin Board of Trustees and all subsidiary board and committees, the development and distribution of Sovrin Open Source Code, the qualification and operation of Stewards, and any revisions to the Sovrin Trust Framework.

2.7 Collective Best Interest

The Sovrin Foundation shall act 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 Sovrin Community as a whole.

2.8 Decentralization by Design

2.8.1 General

The Sovrin Web of Trust shall be decentralized to the greatest extent possible consistent with the other principles herein. As the business, legal, and technical limitations of decentralization may change over time, the Sovrin Foundation shall continuously examine all points of control, decision, and governance to seek ongoing conformance with this principle.

2.8.2 Diffuse Trust

The Sovrin Ledger, Sovrin Network, Sovrin Web of Trust, Sovrin Trust Framework, and Sovrin Foundation shall not concentrate power in any single Individual, Organization, Jurisdiction, Industry Sector, or other special interest to the detriment of the Network as a whole. Diffuse Trust shall take into account all forms of diversity among Identity Owners.

2.8.3 Web of Trust

The Sovrin Ledger, Sovrin Network, and Sovrin Web of Trust shall be designed to not favor any single root of trust, but empower any Sovrin Entity to serve as a root of trust and enable all Sovrin Entities to participate in any number of interwoven Trust Communities.

2.8.4 No Single Point of Failure

The Sovrin Ledger, Sovrin Network, and Sovrin Web of Trust shall be designed and implemented to not have any single point of failure.

2.8.5 Regenerative

The Sovrin Ledger, Sovrin Network, and Sovrin Web of Trust shall be designed so that failed components can be quickly and easily replaced by other components.

2.8.6 Distributive

The Sovrin Ledger, Sovrin Network, Sovrin Web of Trust, Sovrin Trust Framework, and the Sovrin Foundation shall be designed and implemented such that authority is vested, functions performed, and resources used by the smallest or most local part of the Sovrin Community that includes all relevant and affected parties. Deliberations should be conducted and decisions made by bodies and methods that reasonably represent all relevant and affected parties and are dominated by none.[1]

2.8.7 Innovation at the Edge

The continued development of the Sovrin Ledger, Sovrin Network, Sovrin Web of Trust, Sovrin Trust Framework, and Sovrin Foundation shall encourage innovation to take place at the edges of the network among the members of the Sovrin Community most directly involved or impacted.

2.9 Inclusive by Design

2.9.1 General

The design, governance, and operation of the Sovrin Network shall follow the principles of Inclusive Design to serve the widest possible community of Identity Owners.

2.9.2 Identity for All

Consistent with the United Nations Sustainable Development Goal 16.9, the Sovrin Foundation and the Sovrin Network shall promote peaceful and inclusive societies for sustainable development, enable access to justice for all and facilitate effective, accountable, and inclusive institutions at all levels by being accessible to, and inclusive of all Identity Owners without discrimination and with accommodation for physical, economic, or other limitations of Identity Owners to the greatest extent feasible.

2.9.3 People-Centered Design

Sovrin Developers shall put people at the heart of the design process and enable them to control their own user experience.

2.9.4 Design for Difference

[1] Attribution to the Core Principles of Chaordic Commons: http://www.chaordic.org/

Sovrin Developers shall strive to understand differences in capabilities and preferences across all potential members of the Sovrin Community.

2.9.5 Test Across Contexts

Sovrin Developers shall test Sovrin solutions for use in different Identity Owner environments and contexts.

2.9.6 Offer Choice

Sovrin Developers shall design flexibility by offering a choice of ways of achieving the same outcome.

2.9.7 Maintain Consistent Experience

Sovrin Developers shall design comparable experiences that use consistent design elements and language.

2.10 Privacy by Design

2.10.1 General

The design, governance, and operation of the Sovrin Network shall follow the Seven Foundational Principles of Privacy by Design to the greatest extent possible consistent with the other principles herein. These principles can be summarized as:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality - Positive-Sum, not Zero-Sum
5. End-to-End Security - Full Lifecycle Protection
6. Visibility and Transparency - Keep it Open
7. Respect for User Privacy - Keep it User-Centric

2.10.2 Pairwise Pseudonyms by Default

Agents using the Sovrin Protocol shall default to assigning Pairwise Pseudonyms, Pairwise Public Keys, and Pairwise Service Endpoints whenever forming a Connection unless specifically directed otherwise by an Identity Owner.

2.10.3 Selective Disclosure by Default

Issuers, Holders, and Verifiers using the Sovrin Protocol shall default to issuing, holding, and accepting Credentials that support Zero Knowledge Proofs and privacy-respecting Revocation Registries by default.

2.10.4 Trust Framework Disclosure by Default

Sovrin Entities shall by default disclose the Trust Framework under which a Connection is created, an Interaction is performed, or a Credential is exchanged. Agents shall by default notify their Identity Owner of any conflict between the Identity Owner's privacy preferences and the Trust Framework's privacy policies.

2.10.5 Owner Controlled Storage by Default

Agents shall store Private Data in decentralized data storage controlled by the Identity Owner by default.

2.10.6 Anti-Correlation by Design and Default

The design and implementation of the Sovrin Protocol and all components of the Sovrin Network shall avoid any unnecessary correlation.

2.11 Security by Design

2.11.1 General

The design, governance, and operation of the Sovrin Network shall follow the principles of Security by Design to the greatest extent feasible consistent with the other principles herein.

2.11.2 System Diversity

The process and policies for selecting Stewards shall optimize availability and security by maximizing diversity of hosting locations, environments, networks, and systems.

2.11.3 Secure Defaults

The default configuration settings and user experience of the applications using the Sovrin Network and its components shall enforce strong protection by default, including encryption by default.

2.11.4 Least Privilege

Access and authorization of the applications, Agents, and network services that use and comprise the Sovrin Network shall subscribe to the concept of least privilege.

2.11.5 Anti-Impersonation

Applications shall be designed to not allow any party other than the Identity Owner to act as (impersonate) the Identity Owner. Impersonation does not include Guardianship or Delegation.

2.11.6 Accountability

Transactions and application actions that require auditing shall be immutably logged, in a tamper-evident way, and be available to verify processing.

2.11.7 Secure Failure

Applications using the Sovrin Network shall be designed to take an exception or error path that will not create a security weakness exploitable by bad actors.

2.11.8 Pervasive Mediation

Applications shall not assume authorization is transitive across time and/or space—rather security mechanisms shall check every access to every object, and authorize each action on its own merits, just in time.

2.12 Data Protection by Design and Default

Privacy and data protection are separate but related concepts. The right to privacy is enshrined in Article 12 of the Universal Declaration of Human Rights[2] and Article 7 of the EU Charter of Fundamental Rights[3] (the "EU Charter"), while data protection is a fundamental right under Article 8 of the EU Charter. While privacy—and data privacy by extension—have to do with the freedom from interference in the private and family life of an individual, data protection has to do with a specific set of enumerated principles for the protection of an individual's personal data. Data protection is also important when the data belongs to Organizations or Things.

Sovrin Entities, in the processing of personal data, shall adhere to the following data protection principles to the greatest extent feasible consistent with the other principles herein:

2.12.1 Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the Individual.

2.12.2 Purpose Limitation

Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes, shall not be considered incompatible with the original processing purposes.

[2] http://www.un.org/en/universal-declaration-human-rights/ Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
[3] http://fra.europa.eu/en/charterpedia/article/7-respect-private-and-family-life Article 7 - Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications.

2.12.3 Data Minimization

Personal data must be relevant and limited to that which is necessary in relation to the purposes for which it is being processed.

2.12.4 Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that where personal data is inaccurate it is erased or rectified without delay.

2.12.5 Storage Limitation

Personal data must be kept in a form which permits identification of Individuals for no longer than is necessary for the purposes for which the personal data is being processed.

2.12.6 Integrity and Confidentiality

Personal data must be processed in a manner that provides appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures (i.e., information security).

2.12.7 Accountability

Sovrin Entities shall be responsible for and be able to demonstrate compliance with these principles and any other requirements of applicable law.

3 CORE POLICIES

3.1 Stewardship

In keeping with all Core Principles and especially the Decentralization by Design and Security by Design principles:

1. Policies, practices, procedures, and algorithms governing participation of Stewards and operation of Nodes MUST follow all Core Principles.
2. The Sovrin Foundation MUST publish the **Steward Business Policies** as a Controlled Document managed by the Steward Qualification Committee.
3. The Sovrin Foundation MUST publish the **Steward Technical Policies** as a Controlled Document managed by the Technical Governance Board.

3.2 Guardianship

In keeping with the Guardianship principle, a Guardian SHOULD:

1. Act in the Dependent person’s best interest.
2. Exercise good judgment and carefully manage responsibilities.
3. Avoid commingling—keep Dependent’s property separate (e.g. separate DIDs, Public Keys, Wallets, Vaults, etc.).
4. Keep detailed records of all actions taken on behalf of the Dependent.
5. Not violate the Anti-Impersonation principle (section 2.11.5).
6. Be subject to applicable legal structures regarding the granting and revocation of Guardianships.

3.3 Inclusion

In keeping with the Inclusive by Design principles:

1. Access to the Sovrin Network MUST be open to all Individuals and Organizations on a comparable basis without intentional exclusion of specific persons or communities.
2. Developers SHOULD design for different capabilities in different contexts considering:
    a. Digital Exclusion (e.g., access to connected devices)
    b. Physical or Cognitive Exclusion (e.g., disability or incapacity)
    c. Political & Social Status (e.g., stateless individuals; being a child or a woman)
    d. Financial Status (e.g., having no income)
    e. Literacy & Language (e.g., low literacy or not speaking local language)

3.4 Sovrin Web of Trust

In keeping with all Core Principles and especially the Decentralization by Design principles:

1. The Sovrin Trust Framework MUST be designed to provide a foundation for Domain-Specific Trust Frameworks (DSTF) based on the Sovrin Web of Trust Model.
2. The Sovrin Foundation MUST publish the **Sovrin Certification and Accreditation Policies** as a Controlled Document managed by the Sovrin Trust Framework Working Group.
3. The Sovrin Certification and Accreditation Policies MUST include the technical specifications for all Credential Definitions required for Self-Certification and Accreditation of all Sovrin Web of Trust Roles.
4. The Sovrin Foundation MUST publish a DSTF, the **Sovrin Directory Trust Framework**, whose purpose is to provide decentralized cryptographically-verifiable directory services for DSTFs.
5. The Sovrin Certification and Accreditation Policies MUST be designed to enable any qualified Auditor Accreditation Body to accredit Auditors for the Sovrin Domain Trust Framework.
6. A Sovrin Entity serving in one of the Sovrin Web of Trust Roles who conforms to the Sovrin Certification and Accreditation Policies MAY use the appropriate Sovrin Trust Mark as specified therein.

3.5 Economics

In keeping with the Sustainability principle:

1. The Sovrin Foundation MUST manage the Sovrin Token to ensure economic viability and sustainability for the Sovrin Ledger, Sovrin Network, and Sovrin Web of Trust in keeping with its charter as a non-profit public trust organization.
2. The Sovrin Foundation MUST publish the **Sovrin Token Policies** as a Controlled Document managed by the Economic Advisory Council.
3. Transactors MUST have write access to any of the publicly available Transaction Types for the Main Ledger and the Payment Ledger provided the Entity includes the associated Ledger Fee for the Transaction Type as specified in the Ledger Fee Table stored on the Config Ledger.
4. The Economic Advisory Council MUST determine the Ledger Fees subject to approval by the Sovrin Board of Trustees.

4 GOVERNANCE

The Sovrin Trust Framework and its Controlled Documents shall be revised from time to time as the Sovrin Ledger, Sovrin Network, and Sovrin Web of Trust grow and evolve. The policies in this section govern this revision process.

4.1 General

1. The Sovrin Foundation MUST publish **Sovrin Governance Bodies** as a Controlled Document managed by the Governance Committee.
2. The Governance Committee MUST recommend revisions to the governance policies in this section (Section 4) of the Sovrin Trust Framework. Any such revisions MUST be approved by the Sovrin Board of Trustees.

4.2 Revisions to the Sovrin Trust Framework

These policies apply to the present document (the STF).

1. Revisions to the STF MUST respect the Purpose and Core Principles.
2. The commencement of any revision process MUST be publicly announced by the Sovrin Foundation no later than the time of commencement.
3. Participation in the revision process MUST be available to all members of the Sovrin Community.
4. Proposed revisions MUST be subject to a minimum 30 day public review period publicly announced by the Sovrin Foundation.
5. Revisions MUST be approved by a supermajority vote of at least two-thirds of the Sovrin Board of Trustees.
6. Prior to the next major revision of the STF, the Sovrin Foundation MUST put in place new governance policies that implement the Sovrin Decentralization by Design principles.

4.3 Revisions to Controlled Documents

These policies apply to the Controlled Documents listed in Appendix A.

1. A Controlled Document and/or the list of Controlled Documents in Appendix A MAY be revised independently from the present document.
2. A Controlled Document MUST have a designated governing body listed in the **Sovrin Governing Bodies** document.
3. A Controlled Document MUST be stored in and use the change control mechanisms established by the official Sovrin Foundation code repository at the permanent location for the document published in Appendix A.
4. Proposed revisions MUST be subject to a minimum 30 day public review period publicly

announced by the Sovrin Foundation.

5. Revisions to a Controlled Document MUST be approved by the Sovrin Board of Trustees after the conclusion of the public review period and before the revision takes effect.

5 APPENDIX A: CONTROLLED DOCUMENTS

The following Controlled Documents are normative components of the Sovrin Trust Framework V2. See section 4.3.

5.1 Definitions

Document Name	Description	Governed By	Normative Location
Sovrin Glossary	Definitions of all terms used in the STF	Sovrin Trust Framework Working Group	Google Doc Version Final location will be: https://sovrin.org/library/glossary/
Sovrin Governing Bodies	Definitions of governing bodies within the Sovrin Foundation	Sovrin Board of Trustees	Google Doc Version
Sovrin Ledger Transaction Data	Defines the data and metadata process by a Steward Node	Technical Governance Board	Google Doc Version

5.2 Specifications

Document Name	Description	Governed By	Normative Location
Decentralized Identifiers 1.0	Specification for DIDs and DID documents	W3C Credentials Community Group	https://w3c-ccg.github.io/did-spec/
Sovrin DID Method 1.0 Specification	Specification for DIDs on the Sovrin Ledger or Sovrin Microledgers	Technical Governance Board	[Permanent link] https://github.com/sovrin-foundation/sovrin/blob/master/spec/did-method-spec-template.html
Verifiable Credentials Data Model 1.0	Specification for verifiable credentials	W3C Verifiable Claims Working Group	https://w3c.github.io/vc-data-model/

5.3 Policies

Document Name	Description	Governed By	Normative Location
Sovrin Steward Business Policies	Governs Steward qualification, enrollment, and operational status	Steward Qualification Committee	Google Doc Version
Sovrin Steward Technical Policies	Governs the technical requirements for operating and protecting a Node	Technical Governance Board	Google Doc Version
Sovrin Token Policies	Governs token minting, mining, allocation, fees, etc.	Economic Advisory Council	Google Doc Version
Sovrin Certification and Accreditation Policies	Defines certification and accreditation programs for all STF Roles	Sovrin Trust Framework Working Group	Google Doc Version