The Principles of SSI

These foundational principles of SSI are intended for use by any digital identity ecosystem. Any organization is welcomed to incorporate these principles into its digital identity ecosystem governance framework provided they are included in their entirety. The principles of SSI shall be limited only by official laws and regulations that apply in a relevant jurisdiction.

1. Representation

An SSI ecosystem shall provide the means for any entity—human, legal, natural, physical or digital—to be represented by any number of digital identities.

2. Interoperability

An SSI ecosystem shall enable digital identity data for an entity to be represented, exchanged, secured, protected, and verified interoperably using open, public, and royalty-free standards.

3. Decentralization

An SSI ecosystem shall not require reliance on a centralized system to represent, control, or verify an entity's digital identity data.

4. Control and Agency

An SSI ecosystem shall empower entities who have natural, human, or legal rights in relation to their identity ("*Identity Rights Holders*") to control usage of their digital identity data and exert this control by employing and/or delegating to agents and guardians of their choice, including individuals, organizations, devices, and software.

5. Participation

An SSI ecosystem shall not require an identity rights holder to participate.

6. Equity and Inclusion

An SSI ecosystem shall not exclude or discriminate against identity rights holders within its governance scope.

7. Usability, Accessibility, and Consistency

An SSI ecosystem shall maximize usability and accessibility of agents and other SSI components for identity rights holders, including consistency of user experience.

8. Portability

An SSI ecosystem shall not restrict the ability of identity rights holders to move or transfer a copy of their digital identity data to the agents or systems of their choice.

9. Security

An SSI ecosystem shall empower identity rights holders to secure their digital identity data at rest and in motion, to control their own identifiers and encryption keys, and to employ end-to-end encryption for all interactions.

10. Verifiability and Authenticity

An SSI ecosystem shall empower identity rights holders to provide verifiable proof of the authenticity of their digital identity data.

11. Privacy and Minimal Disclosure

An SSI ecosystem shall empower identity rights holders to protect the privacy of their digital identity data and to share the minimum digital identity data required for any particular interaction.

12. Transparency

An SSI ecosystem shall empower identity rights holders and all other stakeholders to easily access and verify information necessary to understand the incentives, rules, policies, and algorithms under which agents and other components of SSI ecosystems operate.

This document was developed by members of the global SSI community as convened by the Sovrin Foundation as a steward of these Principles.

This document is maintained by the Sovrin Foundation and has been approved by the Sovrin Board of Trustees for inclusion in the Sovrin Utility Governance Framework and the Sovrin Ecosystem Governance Framework.

We invite you to contribute any comments or suggestions to the living community version of this document—access is open to anyone.

If you are interested in participating in ongoing development of these Principles of SSI, please visit the Sovrin Governance Framework Working Group Meeting Page.

The Principles of SSI are endorsed and supported by: