Principles of SSI

Version 1.0
19 May 2021

This publicly available recommendation was approved by the ToIP Foundation Steering Committee on 19 May 2021.

The mission of the Trust over IP (ToIP) Foundation is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. Founded in May 2020 as a non-profit hosted by the Linux Foundation, the ToIP Foundation has over 300 organizational and 100 individual members from around the world.

Please see the end page for licensing information and how to get involved with the Trust Over IP Foundation.

Table of Contents

Document Information

Author

Chris Raczkowski
Drummond Reed, Evernym
Sankarshan Mukhopadhyay, Dhiway Networks

Acknowledgements

The Principles of SSI are a set of foundational principles created at the Sovrin Foundation through a consultative process with the SSI community. These principles have been published under a CC BY-SA 4.0 license.

Revision History

Version	Date Approved	Revisions
1.0	19 May 2021	Initial Publication

Terms of Use

Executive Summary

A design principle is a proposition or value that informs, guides, and constrains the design of a product, service, or system.

The Principles of SSI Task Force present this set of principles in order to establish a clear understanding of SSI technologies when used in context of a software system. These design principles are for formal reference by Governance Frameworks which are based on the Trust over IP (ToIP) Governance Framework Metamodel. Additionally, the Principles of SSI are available for any digital trust ecosystem which chooses to incorporate these principles.

When read together as an indivisible collection of principles, these enable a clear understanding of the digital trust ecosystem based on SSI technologies.

Introduction

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.

The Principles of SSI should serve as an informative guide to organizations implementing SSI based systems. The Principles do not represent a compliance standard. They emerged out of extensive conversations with participants in the SSI community. These conversations revealed different levels of understanding around the aspects of SSI and so these principles help to address these gaps.

Purpose

This document provides emerging ecosystems, organizations and individuals with a clearly defined set of design principles which encapsulate the core tenets of SSI. These principles are designed and laid out in a manner that enables a richer and deeper understanding of SSI and addresses the challenges emerging from misuse or wrong use of SSI in order to explain technology choices around digital identity.

The Principles of SSI

Listed below are a set of 12 foundational principles of SSI. These are accompanied by explanatory text to aid in easier understanding of the applicability of the principles in any digital identity ecosystem

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 & 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

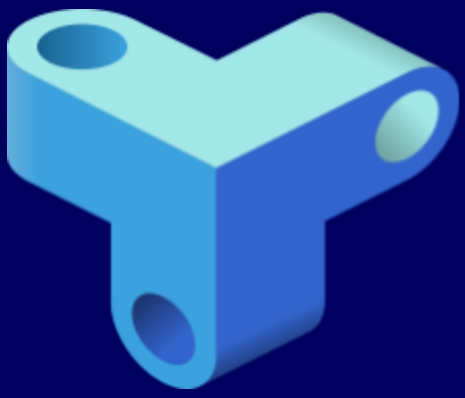
An SSI ecosystem shall empower identity rights holders to provide verifiable proof of the authenticity of their digital identity data.

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.



TRUST Over IP FOUNDATION

The Trust Over IP Foundation (ToIP) is hosted by the Linux Foundation under its Joint Development Foundation legal structure. We produce a wide range of tools and deliverables organized into five categories:

- Specifications to be implemented in code
- Recommendations to be followed in practice
- Guides to be executed in operation
- White Papers to assist in decision making
- Glossaries to be incorporated in other documents

ToIP is a membership organization with three classes—Contributor, General, and Steering.

The work of the Foundation all takes place in Working Groups, within which there are Task Forces self-organized around specific interests. All ToIP members regardless of membership class may participate in all ToIP Working Groups and Task Forces.

When you join ToIP, you are joining a community of individuals and organizations committed to solving the toughest technical and human centric problems of digital trust. Your involvement will shape the future of how trust is managed across the Internet, in commerce, and throughout our digital lives. The benefits of joining our collaborative community are that together we can tackle issues that no single organization, governmental jurisdiction, or project ecosystem can solve by themselves. The results are lower costs for security, privacy, and compliance; dramatically improved customer experience, accelerated digital transformation, and simplified cross-system integration.

To learn more about the Trust Over IP Foundation please visit our website, https://trustoverip.org.

Licensing Information:
This Trust Over IP Foundation deliverable is published under the following licenses: