DIDAS Good SSI Practices[1)]

Right for digital Identity, freedom of choice and portability.

Ability to Delegate / Guardianship

High data protection with minimal disclosure

Coercion-free and self-sovereign

User-friendly with added value

Safely decentralized

Transparent interoperability

Trust in data and information

1) In Anlehnung an WEF – Identity in a Digital World A new chapter in the social contract (WEF_INSIGHT_REPORT_Digital Identity.pdf (weforum.org)), Christopher Allen – The Path of Self-Sovereign Identity (The Path to Self-Sovereign Identity (lifewithalacrity.com)) und Sovrin – Principles of SSI (Principles of SSI – Sovrin)

Summary of SSI Practices[1] – 1/2

Right for digital Identity, freedom of choice and portability.

The SSI ecosystem ensures that every entity (people, companies, objects, etc.) can be represented in the virtual space by one or more digital identities (inclusion). The entity should be granted the right to freedom of choice and decisions should not have a discriminatory effect. This freedom of choice also includes the right to a barrier-free change of provider.

Coercion-free and self-sovereign

The SSI ecosystem ensures that entities can freely reveal their identity or parts of it. Furthermore, it enables the use and release of digital identity data to be carried out by the owner in a controlled manner. The identity owner has full transparency of what he/she has shared with whom and can delete or update his identity data and relationships at any time.

Ability to Delegate / Guardianship

The SSI ecosystem ensures that entities are enabled to delegate the representation and use of their identity to third parties (other people, organizations, devices, etc.). In particular, it ensures that people who are disabled or not of age do not experience any disadvantage.

User-friendly with added value

The SSI ecosystem ensures that the application of the digital identity is simple, intuitive and consistent. It should not only focus on partial aspects (e.g. authentication) but should provide the owners with comprehensive added value. An ability to use in multiple situations (frequency) contributes to an increased attractiveness - and vice versa.

[1] Adapted from WEF – Identity in a Digital World A new chapter in the social contract (WEF_INSIGHT_REPORT_Digital Identity.pdf (weforum.org)), Christopher Allen – The Path of Self-Sovereign Identity (The Path to Self-Sovereign Identity (lifewithalacrity.com)) and Sovrin – Principles of SSI (Principles of SSI – Sovrin)

Summary of SSI Practices[1] – 2/2

Safely decentralized

The SSI ecosystem ensures that the participants are not dependent on a central system. There is no central authority that generates digital data without the consent of the identity holder ("shadow information"), organizes, controls or verifies the exchange. The SSI ecosystem enables owners to save data and transactions, manage cryptographic features (identifiers, keys) themselves and establish encrypted communications with the other owners.

Transparent interoperability

The SSI ecosystem ensures that the request and storage, presentation and exchange as well as the verification of identity data within the ecosystem and in interaction with other ecosystems are designed to be interoperable and transparent. All participants should have the right to gain insight into the necessary information so that they understand the conditions under which the ecosystem works. This is made possible by the application of uniform, open and international standards.

High data protection with minimal disclosure

An SSI ecosystem ensures that the entity's privacy and integrity are always protected, that unauthorized third parties have neither access nor insight into the identity data and its use (privacy by design) and that the identity holders have to disclose only the part of the data that is required for the Business application/transaction in question.

Trust in data and information

An SSI ecosystem ensures that there is trust between the participants. Identity holders should be able to present identity data in a tamper-proof manner. Recipients of identity data should be able to check the authenticity of the data they receive to ensure that they come from an authorized source.

[1] Adapted from WEF – Identity in a Digital World A new chapter in the social contract (WEF_INSIGHT_REPORT_Digital Identity.pdf (weforum.org)), Christopher Allen – The Path of Self-Sovereign Identity (The Path to Self-Sovereign Identity (lifewithalacrity.com)) and Sovrin – Principles of SSI (Principles of SSI – Sovrin)