esatus

Wisdom and Merits Delivered by the 12 Principles of SSI.

07
21

The 12 Principles of SSI

https://sovrin.org/principles-of-ssi

Last year, the global SSI community got together and, convened by the Sovrin Foundation, formulated "their" 12 Principles of SSI. Rightfully, the Principles got immediate recognition and acceptance. We at esatus are still very grateful for this effort, as from this point on we had clear guidelines for what we always referred to as "True SSI". What we wanted to do for a long time: Confirm why and how esatus and its SSI solutions are in accordance with the 12 Principles of SSI.

Now is definitely a good moment to do exactly that. The global momentum for getting SSI in productive applications is ever growing. Obviously, this is a good thing and exactly what the community has been hoping and working hard for. As expected, a lot of players who enduringly declined their interest are now waking up, desiring to board the SSI train. Formulated a bit more pointedly, all the birds of prey (or vultures?) are now rising to obtain their share of the game. This can be – and luckily often is – a good thing, as it helps growing the SSI ecosystem(s) and fostering broad SSI adoption. It can come with a downside when those debutants try to sell their unchanged business model as SSI. A behavior which in the community is known as "SSI washing".

Taking the 12 Principles of SSI as foundation and using esatus as an example, we illustrate how anyone can do their own vetting if they are dealing with "True SSI" organizations and products. A few cornerstones to keep in mind when taking in the analysis:

Our esatus SSI solutions...

- are embracing decentralized identifiers (DIDs) and verifiable credentials (VCs),
- are based on the proven open source Hyperledger Aries and Hyperledger Indy technology stack,
- support well-known ledgers like Sovrin and IDunion out-of-the-box,
- are production grade and built for enterprise use,
- are supported, maintained, and continuously enhanced, with designs being adapted for newer SSI streams.

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.

Peer-to-peer DID connections are key characteristics of the underlying technologies, making representation by many digital identities the default. This means: Every new “handshake” between entities spawns a new DID on both ends, with a unique peer-to-peer connection.

The technology set is currently best established for human, legal and digital entity use. Together with the global community, esatus is already working on adapting it for natural and physical entity use cases (e.g. site access, IoT).

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.

The identity infrastructure technologies are free and open source, designed with interoperability in mind. To interoperate between identity ledgers, the community has converged to establishing DID methods which are “routable” to the correct ledger. For Hyperledger Indy ledgers, the required DID method (DID: Indy) is currently in the making. Recognized, royalty-free standards for VCs are created by the W3C (World Wide Web Consortium), a roadmap for achieving W3C compliance of VCs in Hyperledger Indy is in the making. VC schemas can be created by the VC providers freely themselves. esatus provides a Hyperledger Aries compliant wallet app free of charge for Android and iOS devices (and will continue to do so).

Providing, maintaining and operating backend components enabling business logic and ledger interactions as well as supporting clients with their SSI projects are paid-for products/services. Clients can choose alternative vendors for SSI components at any time, swapping the esatus tech stack while still using the same VC logic. They can even build and maintain the backend themselves. esatus is convinced to have attractive products and services in its portfolio, giving no reasons for moving away. esatus products are constantly improved based on client feedback.

3. Decentralization

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

The infrastructure tech stack is fully decentralized, with diversity in node operations being not only possible but desired in Hyperledger Indy network setups. Open and inclusive governance models for ledgers are the norm and no SSI org could prevail in a closed-shop, restrictive mode. VCs and proofs can freely float: Holders can hold and present what they want, issuers can issue what they want, verifiers can request and verify what they want, and the latter two may ask a fee for their services. Organizations using SSI can freely determine and change their ledger of choice. An organization will need their own backend and institutional wallet for SSI enablement, in an operation and maintenance mode fitting their needs.

esatus backend solutions can be Software-as-a-Service or dedicated client installations, on the cloud platform of choice or on premises. Clients can always use the underlying SSI infrastructure without any restrictions.

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.

These requirements are met by the underlying technologies by design, they are centered around the user (holder) and empower her in unprecedented fashion. Holders decide if they want to make data accessible on each request, using the wallet they choose, and which they can change at any time. Wallet interoperability including backup and synchronization has been identified by the global SSI community as a key work item.

Holders may even opt for a wallet hosted in the cloud, which is not recommended by esatus as well as many of the SSI community. Guardianship exercised by an individual or an organization is an enthusiastically worked on domain, e.g. by the Sovrin Guardianship working group. Technological underpinnings for guardianship are admittedly not yet there.

5. Participation

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

There is no mandatory participation in any of the SSI ecosystems esatus is involved in. Enabling populations who are not willing or able to participate with the required digital means is a key concern of the SSI community. Technology-less ways for SSI enablement – e.g. “paper credentials” – are a dedicated topic of a highly motivated subgroup.

In general, esatus’ viewpoint is that participation in the established SSI use cases and networks is very attractive and beneficial for everyone. The large-scale SSI use cases which esatus helps to unlock are designed with maximum inclusivity and properly addressing the digital gap in mind. SSI is for everyone and makes all our digital lives easier and safer. esatus promotes this recognition and perception and contributes with both broad education and easy-to-use technology.

6. Equity and Inclusion

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

The SSI ecosystems esatus is involved in are open for everyone within their governance scope and all participants are treated equally. There are no logical prerequisites for participation. Some use cases are built around certain jurisdictions or governmental use cases, which means they are targeted at a specific group of people, e.g. citizens of a state or country. This is a deliberate target group restriction but not an SSI limitation. From a technical perspective, SSI facilitates entry points for those who are less tech-savvy or not equipped with the necessary technical components (see 7).

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.

The esatus SSI solutions are optimized for efficiency and effectiveness, for both organizational backend components and digital tooling facing individuals, such as wallet apps. Continuous optimization of user experience, convenience and usability is baked into the esatus software development lifecycle. Enhancing the baseline technology an individual identity rights holder needs for SSI – a wallet app – with more accessibility features is on the esatus development roadmap.

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.

Flexibility is a key design requirement for esatus, i.e. our SSI solutions have built-in data portability functionality. Backend components, institutional wallet and holder wallet app allow data backups, configurable and executable by the administrators/users themselves. esatus highly recommends backups of all org/user data on a frequent basis. For the wallet app, an automated backup in a storage of the user's choice is on the esatus development roadmap. For enterprise environments, policy settings will be possible for corporate wallet apps rolled out to employees. Policies will enable configuration of mandatory automated backups, and restricted functionality if backups are not performed within a defined timeframe (e.g. no new credentials can be accepted if the backup was not run for 24+ hours).

Holders decide which wallet they would like to use, and which they can change at any time. Wallet interoperability with backup/restore across different wallets has been identified by the global SSI community as a key work item. esatus goes even further by promoting an automated synchronization between all wallets apps a holder would like to use in parallel. Synchronization is on the mid-term esatus development roadmap, which requires standards definition with the global SSI community.

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.

Enforcing information security has been esatus' claim for many years and remains the foundation of what esatus stands for. Embracing and deploying IT security standards and best practices is mandatory in all esatus SSI solutions. End-to-end encryption of all communications between actors and agents (data in motion) is already a key characteristic of the underlying SSI infrastructure technologies. SSI empowers users (holders) but also makes them responsible for securely storing their identity data and private keys (data at rest). A fundamental responsibility for us as SSI technology providers is creating adequate technical means for keeping a holder's private keys safe. Biometric protection of the wallet app, storing all data only in encrypted fashion and leveraging available secure storage enclaves on mobile devices for key material is considered state-of-the-art.

In the past months, esatus has entertained in-depth security reviews with leading German security experts to identify what can be improved further in our own components. This resulted in various immediate security upgrades and a concept for elevated wallet app security which is currently under implementation. This architecture will allow handling of declared "high value credentials", e.g. ID data derived from Government electronic identity cards or insurance policies, in a highly secure manner which was previously unavailable in SSI wallet apps.

10. Verifiability and Authenticity

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

Verifiable proof of authenticity of digital identity data is a key characteristic of the underlying SSI infrastructure technologies, it is the unalterable default and not an option. Digital identity data sets are delivered to an identity rights holder in form of attributes in a verifiable credential (VC). The VC issuer is identifiable by his public DID. A verifier requesting data from a holder via a proof request can, upon data reception, be certain that:

a) the data has been issued to this holder by the publicly identifiable issuer,
b) the data has not been changed since issuance,
c) the VC has not been revoked (revocation is an optional feature when issuing a VC).

Hence all actors in the SSI ecosystem can rely on data being authentic and not having been tampered with. Obviously, trusting the issuer to produce reliable, credible data is a cornerstone assumption in an SSI ecosystem.

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.

Identity rights holders store their digital identity data in their wallet of choice. They are advised to select a wallet which provides a high security standard (see 9) which prevents unauthorized data access. In practical SSI scenarios, selective disclosure of data from VCs is a key characteristic of the underlying SSI infrastructure technologies. For verifiers, it is considered best practice to only ask a holder for the attribute needed for the specific use case (and, in fact, mandated by data protection regulation such as EU-GDPR). Upon proof request by a verifier, a holder is asked for her confirmation to share attributes out of digital identity data stored in her VCs. She can decide if the requested data is relevant for the specific use case and decline the request if it is not. A more elaborate functionality (called "predicates" in SSI terminology) even allows cryptographically assured true/false responses to questions pertaining to numbers, e.g. "Is the account balance above 2,000 USD?". No need for the holder to disclose any more detail – the response is just "true" no matter if her account balance is 2,100 USD or 210,000 USD. In an esatus wallet, a positively answered request can be retracted by the holder at any given time. When interacting with an esatus backend, the standard reaction to those retractions is immediately deleting retained data sets or invoking deletion in connected databases.

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.

The SSI ecosystems esatus is involved in pursuing a transparent, open, and participatory governance model. All relevant procedures and decision structures are documented and made publicly available. The employed SSI infrastructure components are completely built on the open source technology stacks Hyperledger Indy and Hyperledger Aries. The function calls and cryptographic procedures are documented and openly available. esatus SSI solutions are built in full compliance with these open standards, which can be easily verified by interested parties or by just using them with SSI components of other vendors on the same tech stack. Full architectural and interface documentation of paid-for esatus technical components is available for licensed customers or under non-disclosure agreement. If feasible, esatus supports public source code disclosure for transparency, independent security researcher reviews and bug bounty programs.

For the sake of clarity, SSI is a complex topic which one cannot easily fully grasp with a drive-by attitude only. Since 2015, esatus is on a mission to deliver broad SSI education, facilitate in-depth discussion for those who want to dive deep and, more recently, create easy-to-use SSI technology which can be experienced in practical, real-world use cases everyone can relate to.

Publisher: esatus AG

Version: 1.0

Wisdom and Merits
Delivered by the 12 Principles of SSI

esatus stands for a free, secure, and human-centric digital future. We build bridges between today and tomorrow. We shape digitalization processes in a future-oriented way and offer solutions from a single source – from conception to individual software development to operational management.

Another focus is the field of information security (InfoSec). We take a holistic approach when advising companies on the topic of identity & access management and help them to implement compliance and data protection requirements (GRC).

Since 2015, we have been a passionate driver of Self-Sovereign Identity (SSI) in Germany and are now one of the global technology leaders. SSI places the individual at the centre of the digital ecosystem and enables user-friendly and self-determined control of personal data.

esatus