loaha software

Decentralised Self-Sovereign Identity

Existing Identity Systems

Identity is at the core of each and every interaction. While the required level of trust between identities can vary from one interaction to another, the necessity to exchange it in a secure and privacy preserving manner is universal.

Currently there are many different identity systems:

- Public Key Infrastructure (PKI) based identity systems.
- SAML and OAuth Provider (private and government).
- W3C Web Authentication (WebAuthn) standard and the FIDO Client to Authenticator Protocol (CTAP)
- Federated identities such as Google, Microsoft, Facebook, etc.
- .....

=> All are centralized and the user of an identity never owns his data

Decentralised Self-Sovereign Identity System (SSI)

In the self-sovereign identity (SSI) paradigm, individuals and objects are enabled to create and manage their identifiers in a decentralized fashion, without relying on a third-party identity provider.

Unlike existing identity solutions that are structured from the perspective of the organization that provided the identifier (like PKI solutions), self-sovereign identities are structurally set out to work from the perspective of the individual or object that is the subject of a given identifier

=> Self-sovereignty implies that an individual or object who has one or more identifiers or DIDs (Decentralized Identifiers), can present certain Claims or Credentials relating to those DIDs without having to go through an intermediary.

Claims

The mostly used example of a Claim is that an individual is over the age of 18. In the self-sovereign model, such a Claim can either be self-attested (a claim the individual makes about himself) or attested to by another entity (such as the state, eID System or a trust services provider) that can issue an attested claim in the form of a credential to the individual who now becomes the holder of that Credential.

In the latter case the holder is in full control over the previously described Claims and can choose to present a self-attested version of the claim or a Verifiable Credential that has been issued and cryptographically signed by another entity.

With this model of SSI, it is possible to express virtually any kind of claim about an individual or object, and given the adequate verification processes and legal acceptance, these claims can represent anything about the individual or object who is the subject of that credential. This adds a level of flexibility and modularity that will encourage the development of new types of identity claims and will allow a holder to selectively reveal only the relevant data necessary for a given transaction or interaction.

GDPR

SSI is a powerful tool for privacy protection. In fact, it has a strong visionary alignment with the EU's General Data Protection Regulation (GDPR). SSI even has the potential to become the foundation for real world achievement of the GDPR's principles. One objective of the GDPR is to enhance individual data protection rights, just as SSI seeks to provide individuals with more control over their own personal data.

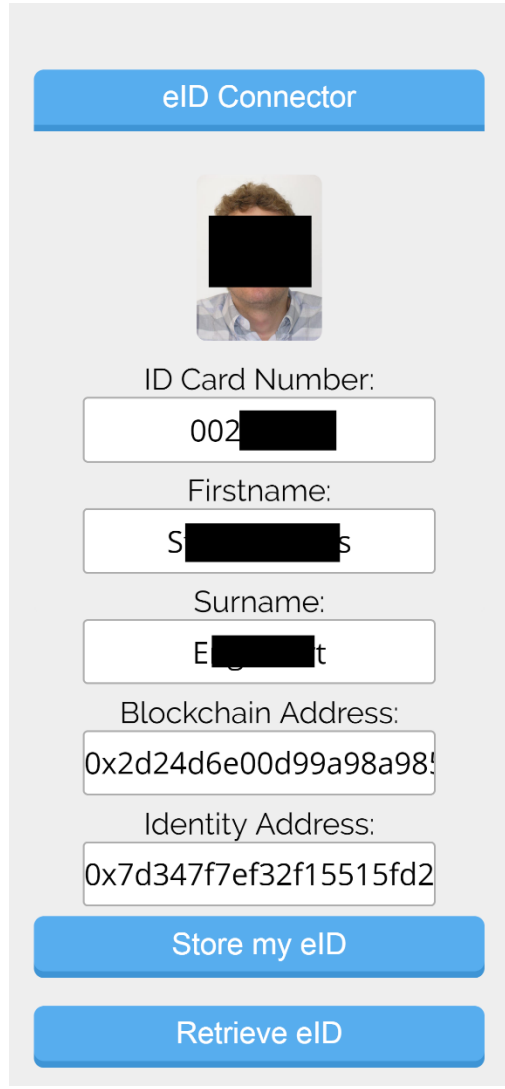
=> For this and many other reasons we need a series of guiding principles to make sure SSI doesn't go rogue. For example Christopher Allen's Ten Principles of SSI as a starting point.

Christopher Allen's Ten Principles of SSI

- Existence — Users must have an independent existence.
- Control — Users must control their identities.
- Access — Users must have access to their own data.
- Transparency — Systems and algorithms must be transparent.
- Persistence — Identities must be long-lived.
- Portability — Information and services about identity must be transportable.
- Interoperability — Identities should be as widely usable as possible.
- Consent — Users must agree to the use of their identity.
- Minimization — Disclosure of claims must be minimized.
- Protection — The rights of users must be protected.

Aloaha's SSI

- Based on ERC and W3C Standards.
- Zero-Knowledge Proofs possible.
- Does not consume Blockchain GAS.
- Connector to Aloaha eForms Server.
- Connector to eID/SAML Provider.
- Connector to Aloaha distributed, immutable storage.
- Aloaha's Identities come with an inbuilt Wallet for payments.
- RFC3161 compliant (eIDAS) Timestamping Server inbuilt.
- Supports ECC and RSA Keys.
- Can be shared with multiple Blockchain accounts.
- **Aloaha SSI already General Available (GA).**



Aloaha software

Use Cases for Self-Sovereign Identities (SSI)

- Archiving of **Call Detail Records** (CDR's).
- **eKYC/KYC** documents can be attached/linked directly with the SSI.
- Companies can attach their public registry documents to their **company identity**.
- Fleet or Aviation Management Systems can give any part an identity to attach **maintenance logs**.
- Contracts and maintenance history can be hold in a **property identity**.
- Patients can finally get back the ownership of their valuable **medical records**.
- Food items can be traced from the production to the consumer.
- Legal Persons can use their SSI as Decentralized Identifier for **Single-Login**.

=> SSI's can act as a single source of truth for many different industries.

Online Resources

- https://www.valletta-coin.com/decentralised-self-sovereign-identity-ssi/
- https://www.valletta-coin.com/aloaha-decentralized-swarm-storage/
- https://www.form-provider.com
- Questions? Just contact info@aloaha.com or call +356 79 567 034

aloaha software

Thank you
info@aloaha.com