Introduction to SSI (Self-Sovereign Identity)

Privacy, customer data, and centralized vs. decentralized storage.

The dusk of legacy Data silos

The way businesses manage user access to their services today relies on the storage of the user information in their databases. This approach is called centralized because it keeps data in the sole control of the business. However, in a majority of cases the data is sold to other companies for some form of business advantage. Furthermore, this is often done based on terms and conditions agreed between a customer and the service provider, whereby the customer grants the provider full ownership of his or her personal information. This agreement allows the provider to sell the data to other companies and monetize it, e.g. through advertising. This is the basis of many business models where the service provided to the customer is given for free. But as the old saying goes, if you're not paying for the product, you are the product! Still, many customers are aware of what happens to their data, and they are fine with this deal. However, there are others who are not comfortable with such a system, and would like to have a choice. At least to make sure that the data is orderly managed once the contract is terminated. The mechanics behind the scene are not very obvious. This is why many legislators brought this issue to the public's attention, and passed new laws regarding privacy and customer data usage. The law forces businesses to explain more explicitly how they handle personal data. As a result, the customer may accept to share all data, or only a specific set of information. This choice needs to be made for every compliant service, e.g. a website. Whilst the laws try to protect the privacy and customer data by providing more transparency, there is currently no focus on solving the issue that all the data is stored in a centralized manner. Even if an individual chooses to not share any of his data to third parties, the data is still stored somewhere in the business's premises, making it prone to theft and misuse from outside hackers. All too often, companies' databases get hacked, leaking thousands, if not millions of usernames and passwords, which pose a major threat to the individual's privacy.

The dawn of Data Sovereignty

There is a trade-off when it comes to data privacy: How can customer data be protected, and how can businesses still be able to use this data to provide their services?
SSI (Self-Sovereign Identity) is a relatively new concept which could reshape the way personal data is stored by providing a faster, more efficient, and user-centric decentralized approach. With SSI, data is stored on the customer side, eliminating many threats stemming from centralized storage. Businesses request the data that is required to provide a certain service on demand, and

customers can choose to share their data if they trust that specific business. Moreover, users manage their data themselves, ensuring that all information they share with businesses is complete and correct. Both the individual, as well as the business benefit from this as it reduces the costs for managing and maintaining user data significantly. This ensures a high level of data protection, and gives complete power to the customer. This is reflected by the new term identity holder which essentially expresses the data ownership of the customer.

The wine shop use case

A simple example will clarify a few aspects on how SSI works and why it will improve data privacy. Think of a wine shop which needs to check if you are old enough to buy a bottle of wine. Currently, in order to prove that you are of legal age, you are required to provide the shop with your identity card or another form of identification. Here, the shop has access to all your data which is visible on your identification document, such as your birth date, your full name, your address, and other sensitive information. This is somewhat too much as all the business requires is a verification that you are above an age of 16 years (as it is in Germany). In this case, none of the additional information viewable on the identification document is necessary, not even your specific birthdate.
With SSI the wine shop can request an age verification digitally and the only thing the business receives is a “Yes” or “No” through the SSI interface of your personal wallet. No other sensitive information is exposed, and the shop doesn't need to spend additional efforts looking through your documents to find out if you are of legal age. The shop can verify your data because that information was issued by a trusted party, for example it was issued by a bank or by the government.

How does SSI solve the centralized data storage problem?

SSI wallets use a similar concept compared to your current physical wallet, but transforms this into digital data records. In your digital wallet you can store your so called verifiable credentials (VCs), which represent some form of validated data about you. Just like in a physical wallet, you own your personal data, and it is stored in your personal digital wallet, completely in your control. In your digital wallet, you can store VCs such as verifiable documents which prove something about you, e.g. your name, address and communication preferences, but also potentially your driver's license, your identification, birth certificate, high school diploma, medical health card, and many more if the respective qualified issuers enter the market. Depending on the level of assurance required these documents can be given to you by authorities (e.g. your driver's license), or by individual businesses (e.g. a membership card for a gym, verifying that you paid your monthly subscription, granting you access to enter the gym).
SSI enables identity holders to control what they share with businesses through the use of VCs, ensuring that only the necessary information is exposed. In addition to improved data management through the use of SSI, the issue of centralized data storage is also tackled with this new technology.

In the SSI ecosystem, the identity holder owns and manages his own VCs. They are stored locally on his device, digitally signed with the personal private keys and the keys of the issuers, guaranteeing that the credentials belong to none other than himself. The VCs can then be sent securely to the businesses to set up or use a service. Here, the information stays in the hands of the identity holder, who simply gives the business permission to view the necessary data. This means that hackers can no longer break into large databases held by businesses to view sensitive data, eliminating many threats for both the user, as well as the businesses.

What about businesses that use my data as a business model?

The idea that businesses do not own your data anymore does not mean they cannot use it. In fact, with the SSI technology, businesses can potentially attract more users as they no longer need to sign up to their service, which we all know can be a long and cumbersome task, and often results in customer churn. Instead, customers simply send the relevant information to the business which is stored securely on their device, and automatically onboarding themselves to the specific service.
Businesses that are used to rely on data as a business model may need to change their data processing flows as they no longer need to hold the sensitive user information in their database. However, the essential information is still available to them. Instead of the burden of managing all the user data, such as: “John Brown, Polka Str. 29, City, State, Country, Married with 3 kids, 40k income, likes shoes”, the business can focus on the relevant information required for a specific task, e.g. to deliver a good. This way, they can still create a good custom experience and even better in fact, as they are provided with more current data. At the same time they no longer risk being hacked which not only destroys the company image, but also puts the individual customers' privacy at risk. For hackers it is much less attractive to tap a data stream for a long timeframe to gather enough valuable data compared to dumping a database within a few seconds.

Do we need special hardware to use SSI?

SSI is about data formats, e.g. to ensure interoperability by using standards, and protocols to interact with other services. So, it is a software-based concept and therefore any modern mobile phone is sufficient to run a software utilizing SSI and depending on the implementation it still can provide a high level of security. To interact with terminals, screens or other people and to protect the data, SSI makes use of the mobile camera, QRCodes, and NFC. That may require phones with these capabilities. To increase the security level and achieve a high degree of convenience mobile phone features like fingerprint sensors, face recognition and other authentication mechanisms are often used to ensure a seamless, secure, and user friendly flow. However, these features highly depend on the respective SSI application or features of a SSI wallet.How do I make sure the person providing a VC is the real owner of the VC?
Holding a Self-Sovereign Identity means to own a decentral identifier (DID). Each SSI data set is linked to a DID of the identity holder. Verifiable credentials (VC) containing data about an identity holder are signed by the issuer with the issuer's private key. The issuer of a VC can be the identity

holder itself of a trusted third party. Any VC will be signed with a private key before sending it to the relying party. The relying party can use the respective decentral identifier (DID) which is part of the verifiable credentials to resolve its public key and find out who signed the VC. If the signature belongs to the identity holder and can be trusted the VC data set belongs to the person providing the information. In fact, only the device of the real owner has access to the private key used for the signature of the VCs and thus, the relying party can be sure the VC was not misused, or tampered with by someone else.

To sum up the benefits of SSI:

- Sign up once and reuse that secured information across multiple services
- User owns and controls his/her own personal information
- Companies always have access to current and valid user information
- Companies can reduce costs for storing and managing user information
- No more centralized data silos for users information