Self-Sovereign Identity (SSI)

Although digitalisation has led to a round of efficiency improvements in business and government processes, it has also created greater risks to privacy and cybersecurity. People and companies are increasingly becoming the victims of data leaks that then allow the leaked personal data to be misused e.g., for phishing and other forms of identity fraud. These problems have sprung up in various domains.

The digitization of the past two decades has led to a more efficient approach for both the government and the business sector, resulting in cost and time savings. However, there are three fundamental concepts that have not been fully integrated into this digitization process: trust, autonomy, and privacy. These concepts are essential for a secure and seamless journey through the digital world.
To establish trust in the digital realm, it often becomes necessary to bridge the gap between the digital and physical worlds, such as the need to make a copy of a passport. This process is not only costly for businesses that require a high level of trust, but it can also be cumbersome for customers, where this physical step may hinder a smooth onboarding process.

Moreover, there is a lack of autonomy over one's data in the digital world. In contrast to a physical passport, which can be presented without the issuer knowing to whom and for what purpose, every transaction in the digital world can be traced by multiple parties, and personal data is collected and stored in databases beyond the owner's control. The 2009 research study titled "**Onze digitale schaduw**" (Our Digital Shadow) already revealed that the data of the average Dutch citizen is present in hundreds to thousands of files, with between 250 and 500 files already attributed to government entities. Given the rapid pace of digitization over the past 15 years, it can be assumed that the number of registrations is now significantly higher than the figures from 2009.

This has led to significant risks to privacy and (cyber)security. Data collections about individuals have become profit centers, and people and businesses are increasingly falling victim to data breaches, after which leaked personal information can be used for activities like phishing and identity fraud. Additionally, data files are interconnected, often leading to unwarranted far-reaching conclusions. Both the recent "**toeslagenaffaire**" and the monitoring of benefit recipients at the **UWV** have seen violations of the principles of privacy law.

A change is imperative in the way we share data, enabling us to regain control over our data and place trust in the data of others in the digital realm. This transformation is known as Self-Sovereign Identity (SSI), a digital identity framework in which individuals or organizations have complete ownership and control over their identities and personal data

SSI: The Digital Identity that works for Individuals

With a digital identity structured according to the philosophy and technology of Self-Sovereign Identity (SSI), you retain control over your data. SSI allows you to navigate the digital world just as anonymously as you desire. Furthermore, the parties with whom you choose to share data can place complete trust in the integrity of this data.
With SSI, we reintroduce three concepts to the digital world that had been forgotten:

Trust

Data pertaining to you, such as your driver's license or passport, is securely encrypted and stored digitally on your mobile device. The authenticity features typically found on physical documents are cryptographically embedded in their digital counterparts. Through these features, one can ascertain the "genuineness" of a digital document. Conversely, phishing emails are becoming increasingly sophisticated, and despite robust education and vigilance, there remains a risk of inadvertently divulging our data to criminals masquerading as trusted entities, such as our bank.
Thanks to SSI, you can automatically verify whether a data request originates from a party that is indeed who it claims to be, via an unforgeable cryptographic certificate. This establishes mutual trust in digital transactions and eliminates opportunities for criminal activities.

Autonomy

In the physical world, the issuer of your passport is unaware of when you present this document to someone. However, in the digital world, this process differs, as seen in cases like logging in with a Facebook or Google account. Unlike a physical passport, third parties in the digital sphere know precisely with whom and when you exchange data. Even the entity providing your data is often notified when you intend to share data, such as during a creditworthiness assessment, sometimes without your knowledge. The autonomy we enjoy in the physical world should also be ingrained in the digital realm.
With Self-Sovereign Identity, you determine what you share with whom. When you authenticate yourself, the issuer of the identity document remains unaware of its usage, akin to how your passport or driver's license presently functions. The validity of these documents can be verified without involving the issuing entity.
Additionally, you can prove your creditworthiness without the involvement of external parties. With SSI, you navigate the digital world with the same degree of autonomy as the physical world, ensuring that no one can observe data exchanges between two parties.

Privacy

In the physical world, often more information is disclosed than strictly necessary. For instance, when checking into a hotel and providing identification, or when proving you are above the age of 18, the inspecting authority obtains information about your physical appearance, full name, date of birth, and, if not redacted, even your Citizen Service Number (BSN). This can change with Self-Sovereign Identity. It allows you to reveal only the information required for a transaction, without exposing the underlying data. For example, you can demonstrate that you are older than 18 without disclosing your birthdate.
Furthermore, you currently share a significant amount of data that companies require to mitigate their risks. Consider, for instance, the income statements from the past few years when applying for a mortgage. With Self-Sovereign Identity, you can demonstrate that your income exceeds the threshold required by a mortgage lender without needing to submit your year-end statements from the past few years.
According to the GDPR, companies are obligated to collect as little data as possible. Thanks to the cryptography underlying Self-Sovereign Identity, evidence can be established regarding the data companies request from you. This enables regulators to verify whether companies adhere to the obligation of data minimization, essentially creating a form of data collection monitoring for businesses. For individuals, this translates to automatic protection against excessive data requests and significant time savings. It is no longer necessary to provide an extensive array of documents, often containing irrelevant data for the specific transaction. Instead, individuals can present only the information necessary for the transaction in a single step.

Unfortunately, introducing Self-Sovereign Identity presents challenges on various fronts. Firstly, the technology has evolved in different directions that lack interoperability, making it challenging to choose how to proceed. Additionally, a successful implementation encompasses more than just technical aspects. Understanding the semantics of digital data, for example, is complex when ecosystem parties are unfamiliar with each other and cannot establish bilateral agreements regarding this data. The issuance of this data is also not straightforward. While many parties are eager to receive data with a high level of trust, it does not automatically mean that providing this data holds intrinsic value for an organization. Lastly, old work methods are often deeply entrenched in existing processes and legal requirements. For instance, regulators prefer to see physical copies when randomly verifying whether parties adhere to established guidelines.

This can and must be improved!

The introduction of SSI is not just a technical challenge but a systemic shift that requires various parties to move together from different angles. That's why Digital Identity is a crucial building block within the DBC, and in 2017, we initiated the SSI Community in collaboration with Digicampus. Through this initiative, DBC facilitates the demand from the field to share knowledge about SSI and exchange experiences. The SSI Community brings together technology partners, implementation partners, and potential clients to collectively work towards creating an interoperable ecosystem.

As part of this effort, we, along with our partners, have defined a technical interoperability profile for SSI known as **DIIP (Decentralised Identity Interop Profile)**. The goal of this interoperability profile is to align with the organizational knowledge level and existing standards, enabling organizations to implement and adopt SSI cost-effectively and seamlessly. When different parties adhere to this same profile, there will be no technical barriers to data exchange.

Interested in becoming part of the SSI Community?

Together with Digicampus, DBC regularly organizes meetings where you can stay updated on the latest developments in SSI, contribute your insights, and collaborate on the interop profile to promote SSI adoption. To stay informed about upcoming SSI Community meet-ups, please reach out to Marc Winsemius at Digicampus via **marc.winsemius@logius.nl**.

SSI Explainer

SSI Explainer

Decentralised Identity Interop Profile (DIIP)

DIIP

DBC newsletter

Sign up for our newsletter and stay informed of the latest news Blockchain

Sign up

DSSIF

Vision document DSSIF | PDF

If you would like more information, please contact:

Alexander van den Wall Bake
Lead Self-Sovereign Identity (SSI)

Contact

Dutch Blockchain Coalition

070-4190309

info@dutchblockchaincoalition.org

o.v.v. Victor van der Hulst

An initiative of

Ga direct naar

Dutch Digital Delta

Use cases

Dutch National Blockchain Course

About us