Introduction to **Self-Sovereign Identity.**

by walt.id

© Version 1.0 [2022] • walt.id • office@walt.id

TL;DR

What is Self-Sovereign Identity?

Self-Sovereign Identity (SSI) **gives people and organizations full control over their data** and allows them to "**bring their own identity**". As a result, SSI enables anyone to prove who they are and potentially anything about them in online and offline interactions.

Why use it?

SSI offers numerous **advantages over traditional approaches to digital identity**, which is true for people and organizations. For example, user interactions become more effortless which creates better experiences for people while minimizing the friction of onboarding for service providers, such as by replacing the need for usernames, passwords, forms or online identification processes. As a result, online fraud and identity theft can be prevented and security improved.

At the end of the day, the **use cases are endless**: From official identity documents required for travel or KYC ("know your customer") to diplomas and certifications required to offer certain services or social information for creating more individual and unique experiences.

Moreover, **Governments across the globe** from the Americas to Europe and APAC and **businesses across industries are adopting this new identity paradigm**. Emerging regulations, like Europe's "eIDAS 2", will even force the adoption of user-centric and user-controlled identity.

How does it work?

From a functional perspective, SSI enables governments and businesses to issue **digital identity documents** to citizens, users and other stakeholders in the form of "Verifiable Credentials". These credentials can be anything (like a passport, diploma or a bus ticket). They are stored and **managed via digital wallets** and **can be reliably verified by anyone they are shared with**.

From a technical perspective, SSI requires a number of concepts (like Trust Registries, keys, Decentralized Identifiers, Verifiable Credentials, authentication protocols) which can be thought of as building blocks that are available in different variations and can be put together in different ways. As a result, there are **different "flavors" or ways to implement SSI** which makes a basic understanding of the technologies particularly important.

How to get started?

Based on our experience, **building a pilot** is the best way to get started and the most effective way to quickly **build-up knowledge** and **prove the value (ROI) of SSI for your organization**.

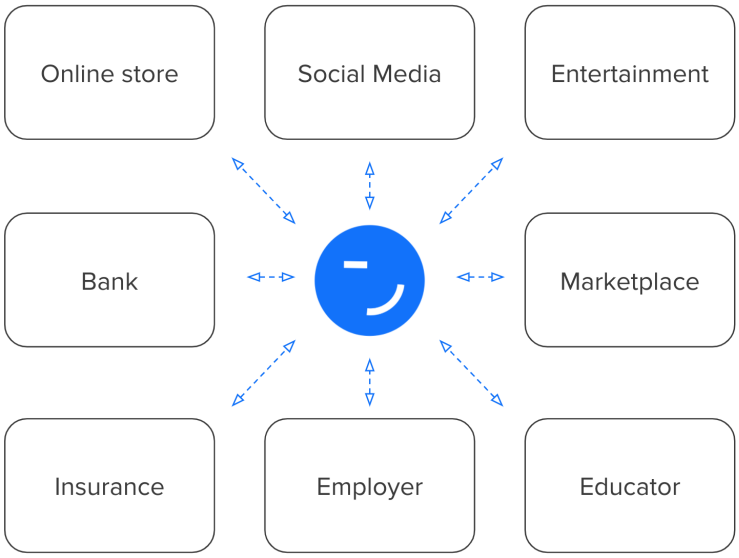
Further Readings

Introductions to Digital Identity and Non-Fungible tokens (NFTs)

What is Self-Sovereign Identity (SSI) ?

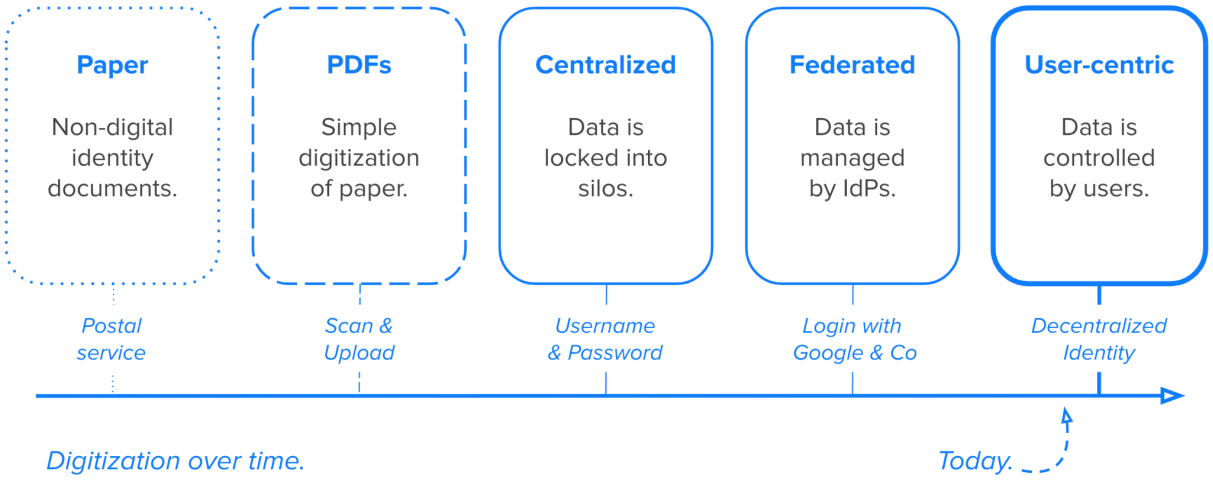
Self-Sovereign Identity (SSI) is a user-centric approach to digital identity that **gives people and organizations full control over their data**. As a result, SSI enables anyone to easily share their data and reliably prove their identity (i.e. who they are and anything about them) without sacrificing security or privacy.

In other words, SSI enables you to "**bring your own identity**" and this is true for potentially any type of information - from your core identity (e.g. name, age, address) to your education and work records, your health and insurance data, bank account and financial information, etc.



Moreover, SSI cannot only be used to model the **digital identities of people**, but also of **organizations** and **things** (IoT).

At the end of the day, SSI promises a digital world in which interactions are effortless and worry-free. It is **simply the next evolutionary step** in identity management, a new paradigm in which our digital identities are no longer fragmented and locked into silos that are under someone else's control, but only at our own disposal to be shared securely and privately.



If you want to learn more about the evolution of digital identity and understand how SSI differs from traditional approaches like Federated Identity ("login with Google & Co"), check out our Introduction to Digital Identity.

Contact us if you have questions or remarks. We're happy to help.

Why use Self-Sovereign Identity?

For a few decades, we are witnessing a process of digitisation that is unfolding globally and across industries. While this process started humbly, it accelerated with the emergence of smartphones which put the digital world in our pockets and more drastically with the outbreak of **COVID** which **forced the world to move from in-person interactions to digital ones**.[1]

However, it is no secret that the **internet was built without an identity layer**, so as the world is growing more digital, **we are confronted with seemingly insurmountable issues.** In other words, while digitisation has many upsides it comes at a price:

- **Lack of control over data**: Power is aggregated in the hands of a few companies, which effectively control data and lock-in users.
- **Privacy issues**: As a result of users not being in control of their data, we witnessed privacy scandals and diminishing trust in data aggregators.
- **Compliance issues**: Online service providers must store and manage user data centrally which opens them up to regulatory scrutiny and penalties.
- **Security issues**: Conventional ways for securing access to services and user data - particularly password-based authentication - proved to be unreliable and caused countless large-scale data breaches.
- **Fraud and identity theft**: Due to the lack of reliable authentication and identification tools, identity theft and other types of fraud are thriving. Online service providers and marketplaces are struggling to ensure trustworthy interactions.
- **Cumbersome user experience**: Users are forced to juggle various authentication methods (inc. many passwords) and go through lengthy online identification processes.

SSI promises to solve these problems by putting users in control of their data and by enabling them to share their data seamlessly, privately, securely and on their own terms.

Value Proposition

SSI has the potential to create massive value for governments, businesses and individuals alike:

Benefits for people

- **User experience**: SSI makes it effortless for people to share their data with others. Traditional approaches for data sharing like forms and uploads are replaced with simple one click experiences.
- **Control**: SSI's user-centric architecture gives people full control over data in terms of storage, access and portability.

[1] *According to McKinsey [1], COVID accelerated the process of digitisation by several years: Today, more than 58% of customer interactions are digital and the majority of products and services are partly or fully digitised. In relative terms, this is a 40% increase in less than 3 years (2018-2021).*

- **Independence**: Being in control of data also means that people are no longer locked in because they enjoy data portability and can take their data with them wherever they go.
- **Trustworthy interactions**: One of SSI's biggest advatages is that it makes potentially any type of data verifiable in order to prevent scams and fraud including identity theft.
- **Security**: SSI mitigates the risk of data breaches or leaks by eliminating major attack vectors such as passwords or the centralized storage of data.
- **Privacy**: The user-centric design of SSI and its support for selective disclosure and other data minimisation techniques ensure privacy.

Benefits for organizations

- **Conversion and stakeholder satisfaction**: Organizations can offer their stakeholders more seamless access to services or products leading to increased conversion rates, decreased help desk requests and overall higher stakeholder satisfaction.
- **Data quality**: SSI enables organizations to receive reliable data about their stakeholders that is verified and signed by trusted third parties.
- **Fraud prevention**: Organizations can prevent various types of malicious behavior ranging from SPAM to identity theft and document forgery.
- **Security**: Organizations can mitigate the risk of or even prevent data breaches by eliminating the risk factors like passwords and aggregated data storage.
- **Compliance**: Organizations comply with privacy and data protection regulations by default due to user-centric data and consent management.

Use Cases

Digital identity is important for every government and every business. There is no sector or industry that would not require it. As a result, the **use cases are endless**.

Examples range from official identity documents required for travel or KYC ("know your customer") to diplomas and certifications required to offer certain services or social information for creating more individual and unique experiences:

Industry	Exemplary Use Cases		
Public Sector	Seamless remote access to eGov services and data provision.	Digitisation of documents (e.g. passports, ID cards, drivers license).	Remote application for / verification of visas, work permits, professional licenses.
Education	Remote student onboarding.	Digitisation of grades lists, diplomas, student IDs.	Facilitation of (cross-border) student mobility.
Employment (Recruiting / HR)	Seamless job applications.	Instant background checks of employees and contractors.	Maintenance of employee and contractor data.
Financial Services	Customer verification (KYC/B).	Remote account opening.	Streamline loan applications / lending.
Insurance	Frictionless customer onboarding.	Seamless access to insurance products, incl. micro-insurance.	Individual insurance rates based on verifiable health data.
eCommerce	Frictionless check-out.	Vouchers, discounts (e.g. for students)	Proof of age (e.g. tobacco, alcohol).
Travel & Mobility	Application / verification of visas.	Hotel booking and check-in/out.	Vaccination proofs, transportation tickets.
Health Care	Proof of insurance.	Digital prescriptions and medical reports.	Proof of vaccination.
Supply Chain	Verification of product authenticity.	Verification of product provenance, lifecycle.	Verification of vendors, other actors.
Marketplaces	Frictionless user onboarding and authentication.	Fraud prevention via user verification and identification.	Automated data provision (right to access).

Adoption

Major players from the public and private sector are adopting SSI, a process that is facilitated by emerging regulations and the global standardization of underlying technologies and protocols:

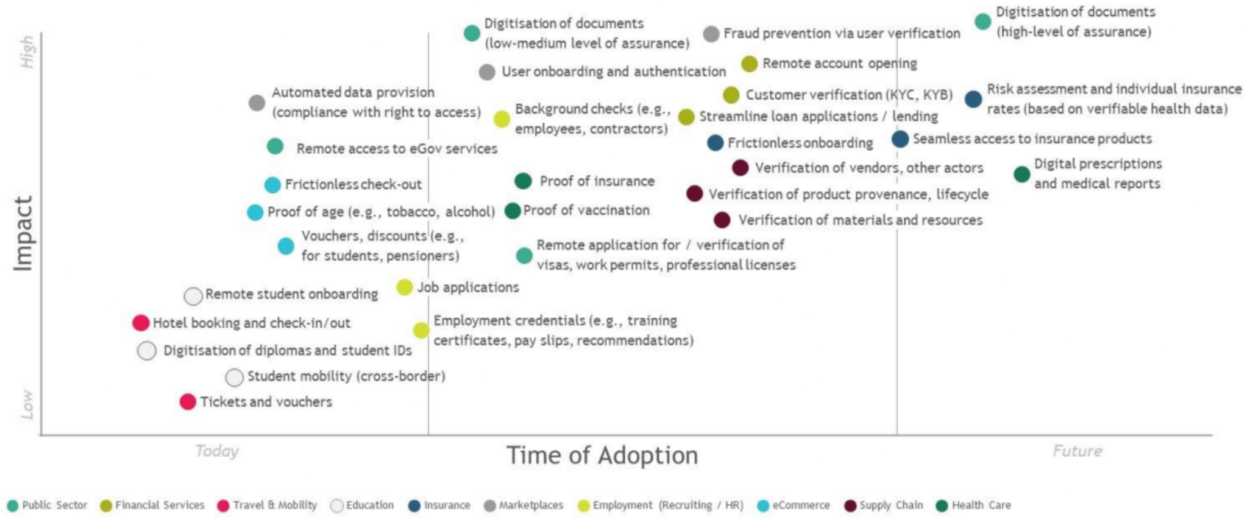
- **Public sector** - Supranational organizations (European Union) and individual governments in Europe, the Americas (US, Latin America) and Asia (APAC) are subsidizing the development of solutions, adapting regulatory frameworks and building pilot projects.
- **Private Sector** - Globally, start-ups, scale-ups and large enterprises are launching projects across almost every vertical, such as banking, financial services, insurance, education, HR/employment, commerce, supply chain, health care, mobility, hospitality, among others.

Selected examples of adopters include:

- **European Union**: The Commission and all Member States have created the “European Self-Sovereign Identity Framework (ESSIF)” and the “European Blockchain Service Infrastructure (EBSI)” which provides standards for a European SSI ecosystem. Moreover, a new regulation called “eIDAS 2” has been announced that will force the adoption of European identity wallets (EUID wallets) and with them a user-centric identity ecosystem.

  Based on these developments, countries like Germany, France, Spain, Netherlands, Belgium, Slovakia, Slowenia, Luxemburg, Lithuania, Greece, Finland, Romania, Croatia are building pilot projects and some are already planning the introduction of production systems within the next 2 years.
- **The Americas**: The United States of America is subsidizing the development of SSI solutions for specific public sector use cases (e.g. visas, customs) via the US Department of Homeland Security. Regional governments in Canada (British Columbia, Ontario) already launched projects (e.g. a public directory of verifiable company data). In South America identity ecosystems such as “LACChain” are emerging.
- **APAC**: Recently, projects in countries like Singapore and Australia became public which further illustrates the global reach of SSI and the fact that public officials understand the advantages of this new identity paradigm as well as their role as drivers of adoption.
- **Private Sector**: On a global level, companies of all sizes started to invest in SSI. Examples include a growing number of banks and financial service providers, tech companies like Microsoft, Workday, Salesforce, SAP and organizations from almost every other industry.

The following graphic *from our* White Paper with the Boston Consulting Group (BCG) shows selected use cases and their expected time to adoption relative to each other:



How it works

To build a mental model of SSI and understand how it works, you must consider two perspectives:

The **functional perspective** which is about understanding the implications of SSI for its adopters and for the market, particularly what SSI enables one to do (that could not be done without SSI).

The **technical perspective**, which is about understanding the technologies on which SSI is built and and their properties which give rise to SSI's functionality in the first place.

Functional perspective

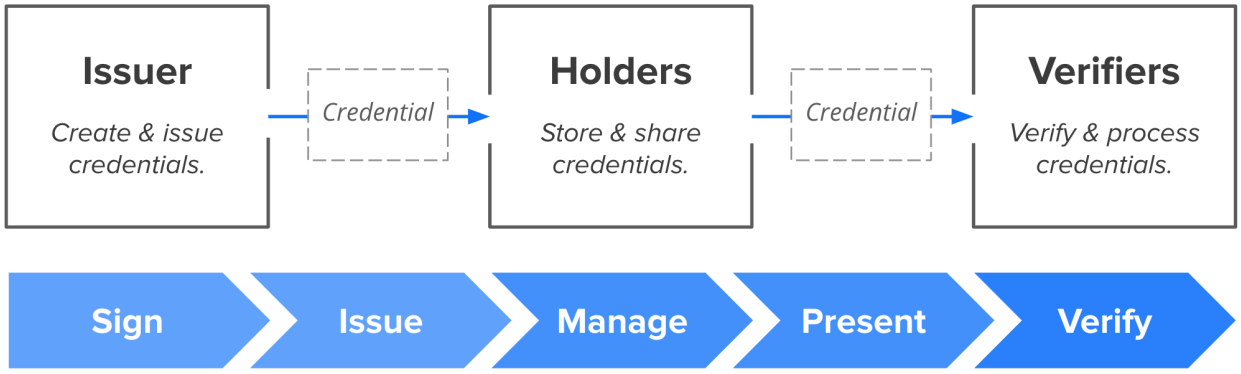
SSI allows us to **model digital identity just like we are used to the way identity works in the non-digital world** based on paper documents and cards. There are just some minor twists.

For example, instead of our identity documents being made of paper or plastic, they are digital credentials made of bits and bytes and instead of storing them in wallets made of leather, they are stored in digital wallets on our phones. Importantly, these digital credentials can be reliably verified by anyone they are shared with online or offline.

In doing so, SSI enables decentralized ecosystems in which different parties can exchange and verify identity-related information. These ecosystems look like three-sided marketplaces, so that every party can take on three roles:

- **Issuers** - Parties who “issue” identity-related data to people or organizations (“Holders”) in the form of digital credentials. They are the original data sources of an SSI ecosystem. *For example, a government issues digital passports to its citizens or a university issues digital diplomas to its graduates.*
- **Holders** - Individuals or organizations who receive digital credentials that contain data about themselves from various sources (“Issuers”). By aggregating and storing such credentials in digital wallets, Holders can build holistic digital identities that are under their control and can easily be shared with third parties ("Verifiers").
- **Verifiers** - Parties who rely on data to provide products and services can reliably verify and process data that has been provided by others (“Holders”). Verifiers, also called “Relying Parties”, are usually organizations or individuals in their professional capacity.

The three roles required for SSI ecosystems:



Note that **a single party can act as Issuer, Holder and Verifier depending on the use case**. *For example, a university may issue diplomas to graduates (Issuer), manage their own accreditations (Holder) and request education records from incoming students (Verifier). You can find more technical information in our documentation.*

Technical Perspective

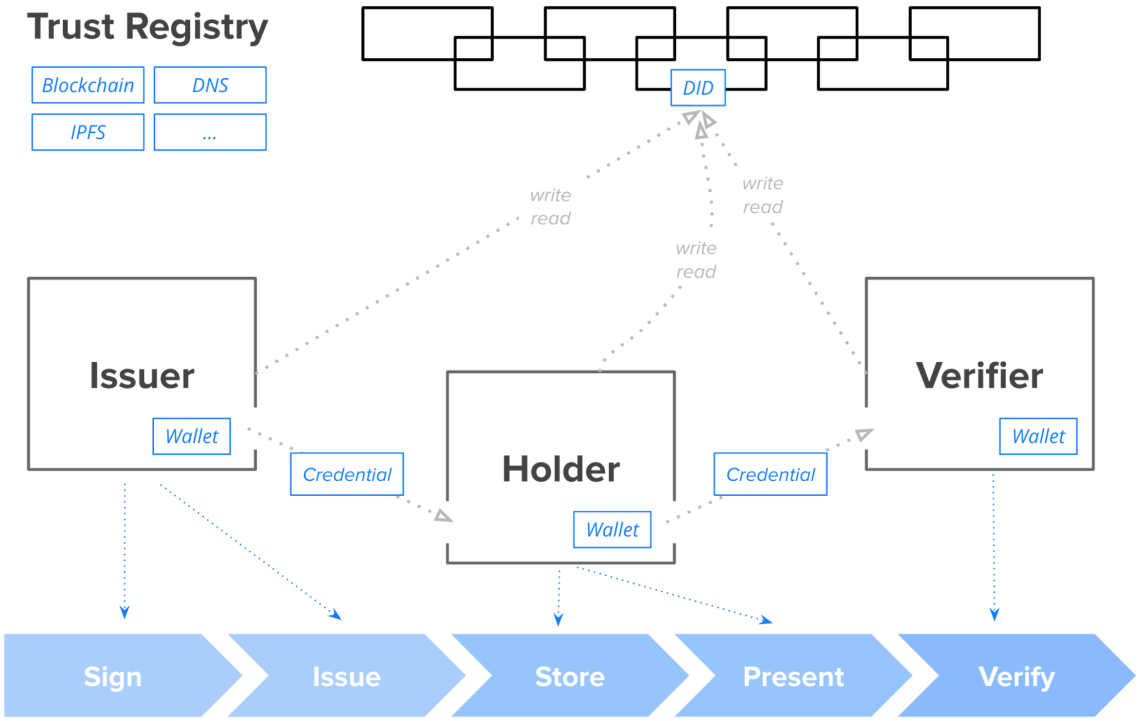
Understanding SSI from a technological perspective requires the understanding of a **few core concepts**:

- **Trust Registries**, which serve as a shared and trusted record of certain information. In other words, they serve as a “layer of trust” and a “single source of truth”.
- **Cryptographic keys**, which convey control over digital identities and enable core functionality such as encryption and authentication.
- **Decentralized Identifiers (DIDs)**, which establish a public key infrastructure by linking keys to unique identifiers that allow different parties to find and interact with each other.
- **Verifiable Credentials (VCs)** which are digital identity documents that can easily and securely be shared with and verified (incl. validity, integrity, authenticity, provenance) by

anyone in a privacy preserving way. Importantly, they are never (!) stored on a blockchain due to privacy and compliance reasons.

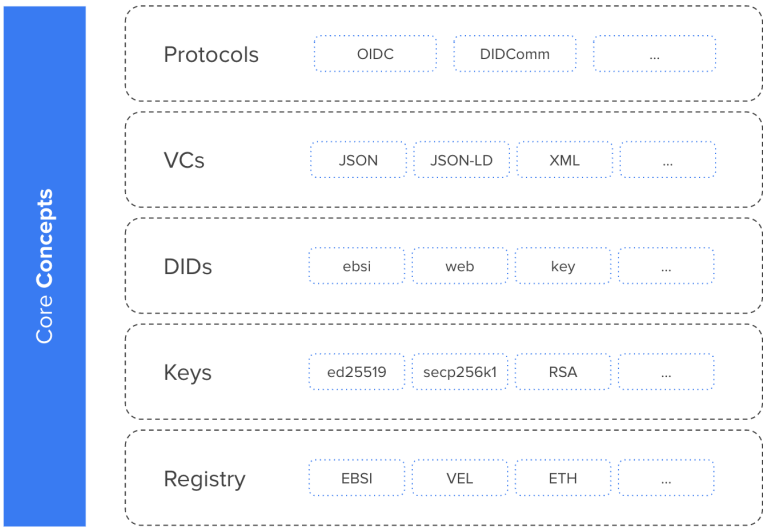
- **Wallets**, which store our keys (control) and VCs (identity data) and enable the management and sharing of our digital identities and data via easy-to-use applications.

The following graphic illustrates how SSI works and highlights the core concepts:



Now, **think of these core concepts as different building blocks** that are **available in different variations** and **can be put together in different ways**. For example:

Different technologies can be used to establish Trust Registries like blockchains (EBSI, Ethereum) or the domain name service (DNS). SSI even works (for certain use cases) without any Trust Registries but purely on a peer-to-peer basis. Similarly different types of DIDs, keys, proofs, credential formats, authentication and data exchange protocols can be used.



Contact us if you have questions or remarks. We're happy to help.

As a result, there are different "flavors" of SSI depending on which variations of which building blocks have been used and how they have been put together.

Importantly, the differences in terms of technologies that are being used illustrate why interoperability has always been one of the most important topics within the industry and why the development and use of **open standards** (e.g. by the W3C, Decentralized Identity Foundation, OpenID Foundation and others) **are vital for technology and vendor selection**.

How to get started?

Based on our experience, the best way to get started is to **collect practical experience by building pilot projects**. This will help you to quickly **build-up knowledge** and **prove the value (ROI) of SSI for your organization**.

To help you with this, we wrote the **Pilot Playbook** which guides you through the process of planning and building pilots with SSI in five steps:

1. **Identify Use Cases**: A framework and examples to help you discover opportunities.
2. **Select Use Cases**: A matrix and different selection criteria will help you analyze and prioritize use cases.
3. **Select an Ecosystem**: An elaboration of ecosystems and a simple approach for selecting the right one for your organization's operating model.
4. **Plan your Implementation**: Guidance on setting project requirements and the technology selection and the question of "buy vs. build".
5. **Implement your Pilot**: Guidance to ensure the successful implementation of your project.

View and download a free copy of the Pilot Playbook.

Walt.id offers developers and organizations an easy and fast way to adopt decentralized identity.

All products are open source (Apache 2), based on open standards (W3C, DIF, OIDF, EBSI) and used by governments, public authorities and businesses across industries (e.g. banking and financial services, web3, education, HR, marketplaces).

To ensure client's success, industry-leading experts provide holistic services from conception over the implementation of pilots and production system to enterprise support and managed cloud services.

For more information visit our website or contact us.

Copyright © 2022 by walt.id GmbH

Contact us if you have questions or remarks. We're happy to help.