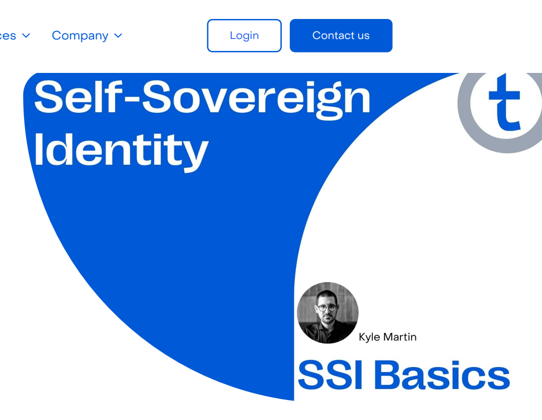
Download our free whitepaper on eIDAS 2.0 and the European Digital Identity Wallet

SSI GUIDE

What is Self-Sovereign Identity?

Learn what SSI is, read about some self-sovereign identity use cases, and how SSI works in this complete overview of SSI technology.



WHAT IS SELF-SOVEREIGN IDENTITY?

Self-sovereign identity explained
Digital identity and blockchain identity management
What is a self-sovereign identity wallet?
SSI in the real world: self-sovereign identity use cases
Key Benefits of Decentralised Identity Solutions
The potential impact of decentralised and self-sovereign identity systems on society
The Truvity APK is your complete SSI solution

Self-sovereign identity explained

Self-Sovereign Identity (SSI) is a digital identity model that enables individuals and organisations to have full control and ownership over their personal data and credentials, without relying on centralised authorities or intermediaries. In this model, the individual becomes the central point of control, and the owner of their identity can manage, share, and revoke access to their data as needed.

With SSI, individuals can securely store their identity information in a digital wallet or container and selectively share it with others as needed, without having to reveal unnecessary or sensitive personal information. By empowering individuals to control their digital identity and personal information, Self-Sovereign Identity aims to enhance privacy, reduce identity theft and fraud, and enable more efficient and secure digital interactions.

How does SSI work?

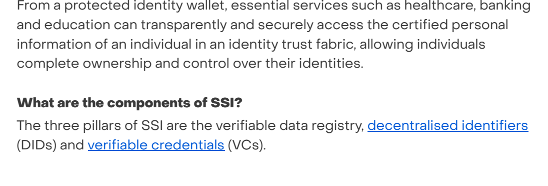
SSI relies on decentralised and/or blockchain-based technologies to ensure that the identity data is tamper-proof and transparent, while also enabling interoperability between different identity systems and platforms. SSI has the potential to transform the way we think about and manage a decentralised digital identity, empowering individuals with greater control over their personal information and protecting them from identity theft and fraud.

At its core, the self-sovereign identity model is a form of decentralised identity, unique in that instead of having a single online identity managed by a third party, SSI users store credentials in digital wallets, that are then made accessible to trusted applications.

From a protected identity wallet, essential services such as healthcare, banking and education can transparently and securely access the certified personal information of an individual in an identity trust fabric, allowing individuals complete ownership and control over their identities.

What are the components of SSI?

The three pillars of SSI are the verifiable data registry, decentralised identifiers (DIDs) and verifiable credentials (VCs).



- **Verifiable Data Registry**: SSI providers connect using a verifiable data registry, with access duplicated and distributed among a multitude of networked computers, that records information in a way that is nigh impossible to hack, cheat or change. This could be implemented using blockchain (by far the most popular method) or through another distributed database.
- **Decentralised Identifiers (DIDs)**: Cryptographically unique, persistent, and verifiable identifiers decoupled from centralised registries or authority. Created by the user and owned by the user, they contain no personally identifiable information.
- **Verifiable Credentials (VCs)**: Digitalised, and cryptographically-secured copies of both paper (passport, driver's licence, etc.) and digital credentials (bank account ownership, credit report, etc.) issued by a trusted third party.

The SSI technology behind decentralised identity

Decentralised and self-sovereign identities are built atop the fundamentals of decentralised technology and cryptography. The core concepts are:

- **Registries**: These hold shared and trusted records of user information, representing a "layer of trust".
- **Cryptographic keys**: Enable core functionality such as encryption and authentication.
- **Decentralised identifiers (DIDs)**: Unique, persistent, and verifiable identifiers that enable the individual to prove their identity without relying on any centralized authority.
- **Verifiable Credentials (VCs)**: Digital attestations or certificates issued by a trusted third party (e.g., an organization, government, or individual) that confirm specific attributes, qualifications, or claims about the identity owner. These credentials can be selectively disclosed, minimizing the risk of oversharing personal information.
- **Verifiable Presentations (VPs)**: Containing identity data for verification from one or more VCs; genuinely created by the user.
- **Trust Frameworks and Governance**: Digital attestations or certificates issued by a trusted third party (e.g., an organization, government, or individual) that confirm specific attributes, qualifications, or claims about the identity owner. These credentials can be selectively disclosed, minimizing the risk of oversharing personal information.
- **Wallets**: Used to store keys and VCs, enabling the high-level management and sharing of digital identity.

Digital identity and blockchain identity management

Distributed Ledger Technology (DLT) is a digital system for recording transactions and asset ownership across multiple sites or participants in a decentralized manner. It relies on a network of computers, called nodes, which work together to validate, record, and synchronise transactions in an immutable and transparent way. Each node maintains a copy of the ledger, ensuring that no single party has control over the entire system. This creates a secure and tamper-resistant record of transactions that can be used in various applications.

The most well-known implementation of DLT is the blockchain, which is the underlying technology behind cryptocurrencies like Bitcoin and Ethereum. In a blockchain, transactions are grouped together into blocks, which are then cryptographically linked to one another in a linear, chronological order. This chain of blocks forms the blockchain, which grows over time as new transactions are added. Consensus algorithms, such as Proof of Work or Proof of Stake, are used by the network to validate and agree on the addition of new blocks to the blockchain.

DLT has potential applications in various sectors, such as finance, supply chain management, voting, digital identity verification, and more. Its decentralized nature can help reduce the risk of single points of failure, enhance security, and improve transparency and trust among participants.

What is identity and access management (IAM)?

Identity and Access Management (IAM) is a framework of policies, processes, and technologies used to manage digital identities and control access to resources within an organization or system. IAM ensures that the right individuals have access to the appropriate resources, at the right time, and for the right reasons. It plays a crucial role in maintaining the security, compliance, and overall efficiency of an organization's IT environment.

Key components of IAM include:

- **Identification**: Assigning unique identifiers (such as usernames) to individuals or systems so they can be recognized within the organization.
- **Authentication**: Verifying the identity of users or systems through credentials, such as passwords, tokens, or biometric data.
- **Authorization**: Determining the permissions and privileges associated with each user or system, defining what resources they can access and what actions they can perform.
- **Access control**: Enforcing the established authorization rules by granting or denying access to resources based on user or system identity and permissions.
- **Auditing and reporting**: Monitoring and logging user activities, access attempts, and changes to permissions for security, compliance, and analytical purposes.

IAM enables users and credential issuers the ability to centrally manage permissions that control access to online applications, software, and resources.

Why is identity and access management important?

Operations leads, Businesses and IT departments are under increasingly strict organisational and regulatory pressures to safeguard corporate resources. As a result of new technologies and new threats, they can no longer rely on the error-prone manual processes previously used to assign and track user privileges.

IAM systems typically involve various tools and technologies, such as Single Sign-On (SSO), multi-factor authentication (MFA), password management, and role-based access control (RBAC), among others. These technologies work together to enhance the overall security of an organization by minimizing the risk of unauthorized access, data breaches, and other security incidents.

By automating these tasks through IAM, businesses are afforded granular access auditing, allowing them to better control their corporate cloud assets.

What is centralised identity management?

Centralised identity management is a framework for collecting, storing and managing a users' identity data in a single location. Dating from the early 2000s when developers realised they needed a way to securely store access information, IAM provides a secure process for identifying, authenticating, and authorising permission for users to digitally hosted accounts, databases and applications through a set of credentials (username and password).

Although not a distinct identity management framework in itself, it is wise to also mention Federated Identity Management (FIM). Seen by many to be the evolution of IAM, FIM is a centralised identity management solution that enables access to applications across multiple domains or entities. For example, a company can give employees one-click access to third-party software like Hubspot or Zoom through a verifying organisation such as Google's "log-in with Google" button.

Centralised vs. Decentralised Identity Management

With centralised identity access management (IAM), users can access all the resources they need with just one login credential. Users must trust A centralised repository to protect and store their personal information and then use those credentials for authentication, authorising them to access multiple accounts, applications and software.

With decentralised identity management, businesses can leverage advanced cryptographic authentication technologies by verifying the identity of users accessing their systems and applications. Providing improved validation, traceability, and documentation, decentralised solutions distribute the end users' digital identity and other credentials over verifiable and secure networks.

Both have advantages and disadvantages. Centralised identity management allows for less user friction and gives organisations more administrative control. However, a poorly implemented centralised system introduces a single point of failure, which critics of the frameworks cite as being the most troubling issue. In 2022, organisations counted their dependency on a single pair of credentials for 82% of all data breaches. Such reliance paves the way for cybercriminals to successfully hack user accounts, gaining access to all the resources that the user is authorised to access.

By switching to a decentralised identity management system such as Truvity, organisations can eliminate that single point of failure by distributing user data and increasing trust. A decentralised IAM relies on nascent Web3 technologies —specifically cryptography and user-owned, decentralised identifiers that allow the user to control their data and offers a convenient way to authenticate themselves through a wide range of applications, while a decentralised ledger such as a blockchain provides secure cryptographic storage.

What is a self-sovereign identity wallet?

Digital identity wallets are used to store keys and VCs, enabling the high-level management and sharing of digital identity, and works through a system of trust:

- **Holder**: The user who generates a decentralised identifier through a digital wallet app, receiving a 'verifiable credential'.
- **Issuer**: An credible organisation then countersigns the verifiable credential with their private key (similar to PGP encryption) and issues it to the holder.
- **Verifier**: A third party then checks the credentials, reading the issuer's public DID on, for example, the blockchain, to verify if the verifiable certificate the holder shared has been signed by the issuer's DID.

As more robust solutions and platforms have developed, making it possible for any developer to learn how to build a self-sovereign identity wallet, there are now a vast wealth of wallets to meet any need.

Download your free copy of "The Past, Present, and Future of Digital Identity" whitepaper

- The costs of traditional systems
- The regulatory demand for change
- Identity systems for every industry
- New and exciting value propositions

Business email* Download

What are the advantages of decentralised identity over centralised?

Decentralised IAM offers a number of advantages over centralised, mainly stemming from it being based on self-sovereign identity blockchain and crypto (hash function) technology. The key ones among these include:

- **Identity Ownership**: With no issuing authority controlling the identity, users create their own decentralised identifiers (DIDs) through blockchain technology, registering and verifying their credentials through the network.
- **Portability/Reusable Identity**: Identity that, once verified, can be ported across multiple apps, websites, software and platforms, scaling down repetitive and heavy onboarding processes.
- **Data Security**: Current verification practices rely heavily on creating huge honeypots of personal data to correlate and verify identity. Businesses can break data up by decentralising it so that no single hack returns enough information to be profitable.
- **Universal Access**: With a unified DID, users can access a wide range of services, accounts, software and platforms through blockchain's ability to provide unified, secure authentication.
- **Cryptographic Storage**: With the blockchain's cryptographic hash function, user information is kept secure with access authenticated through decentralised 'blocks'.

SSI in the real world: self-sovereign identity use cases

Decentralised identity and distributed, verifiable credentials enable users to identify themselves digitally without unduly risking the exposure of personal information, enabling organisations and applications to authenticate access efficiently and allowing a bridge of trust between multiple parties while also remaining compliant with data protection laws and regulations.

Processes that require consent and the sharing of personal data can be managed effectively, with secure connections built between previously unknown users established and stabilised without the need and cost of a credible third party.

Decentralised identity management can be applied to a growing number of use cases including banking and wealth management, government agencies, and eCommerce sites:

Self-sovereign identity in Banking

Financial institutions are constantly grappling with ever-increasing requirements to be more regulated while also remaining flexible to the real-time, 24/7 expectations of their customers. In response to this, banks have turned to the emergence of self-sovereign identity technology development as a solution.

Through a decentralised management kit from a self-sovereign identity solutions provider like Truvity, banks can meet expectations head-on, reducing AML (anti-money laundering costs) through the near-instant, virtual verification of corporate data and ownership and expand their KYC (know-your-customer) offering by allowing users the possibility to open and login to bank accounts in seconds.

Government Agencies

Although many local and national government agencies have already developed eGovernment services, they lack adoption by users due to poor user experience and slow processing times.

A favourite target of hackers (second only to academic institutions), governments are also experiencing more frequent data breaches. Many governments at both local and national levels are exposing themselves to hackers by using antiquated systems, on-site servers and centralised frameworks for information storage.

By implementing decentralised identity technologies and electronic identities (e-ID), governments can ensure trust between providers and clients or consumers, improve turnaround times for national IDs, visas, and other documents, and provide prompt, secure access to essential services such as taxes, voting and business registration without waiting weeks or even months for identity documents to be processed.

eCommerce

A persistent and recurring problem that frequently inconveniences or annoys customers when shopping online is keeping track of usernames and passwords.

eCommerce sites can eliminate this and upgrade their customer experience by utilising a decentralised IAM solution that can provide instant, hyper-secure onboarding and authentication, creating a stress-free customer journey.

Key Benefits of Decentralised Identity Solutions

By leveraging Web3 and cryptographic authentication technology, verifiable identity elements can be hosted across multiple servers, enhancing the integrity of individual identity elements by making them verifiably immutable.

The benefits of adopting a decentralised identity solution are many for individuals, businesses and developers alike.

Why is Decentralised Identity important for individuals?

A decentralised IAM provides individuals with much-needed control over their digital identities through a secure method of log-in, keeping sensitive information on a need to know basis, and more importantly, out of the wrong hands.

For example, the social media giant Meta (formally Facebook) is notorious for its many data breaches. In 2019, 540 million records were exposed in a data leak, including emails, passwords, friend lists, photos, and check-ins. A veritable gold mine for cybercriminals planning social engineering attacks, phishing scams or corporate fraud through Facebook Business Manager.

A decentralised IAM can be used to securely store digital identity, authenticate credentials with encryption, conceal data and greatly reduce the risk of hacks, credential tracking and fraudsters gaining unauthorised access to steal or monetize personal data.

Individuals: Key benefits / takeaways:
- Fully own and control their data
- Prevent device and data tracking as they browse the internet
- Choose who to share their information with

Why is Decentralised Identity important for businesses?

Across all countries, industries and sectors, businesses that implement robust decentralised identity solutions can create long-term competitive advantages and grant themselves several benefits, such as:

- Faster and efficient employee onboarding
- Reduced operational costs
- A frictionless login experience across all channels
- Improved audit trails, supporting compliance

Businesses can realise significant benefits concerning operations, compliance, brand and communications. By saving on operational costs, tech-savvy companies can invest surplus cash into different channels, employee well-being or even build new revenue lines, driving value for both customers and shareholders.

Organisations: Key benefits / takeaways:
- Can better meet GDPR obligations and compliance standards
- HR and operations teams can verify candidate information quickly and efficiently
- By storing less user data, companies can greatly reduce the risk of cyber attacks and fraud

Why is Decentralised Identity important for developers?

A developer adopting a decentralised identity solution into their workflow can expect a range of benefits while allowing them to focus on building user-centric apps that will enhance their digital economies and generate new revenue streams.

By replacing cumbersome sign-up and login processes and removing inefficient authentication procedures and biometric flows, they can eliminate the need for invasive and time-consuming registration processes, such as taking endless photographs of documents and inputting ostensibly pointless information.

Tech-savvy developers using decentralised identifiers can provide end-users access with the click of a button, ensuring both privacy and a seamless user experience.

For applications that require DID and verifiable credentials, developers can utilise a secure SSI solution and implement sophisticated plugin architecture to allow protocols that scale well and interact easily across standards. Such apps will easily be able to verify any identity data, offering users frictionless access to services or products by automating data provision and securely storing, managing and sharing their credentials.

Developers: Key benefits / takeaways:
- Build user-centric apps with seamless sign-up processes
- Eliminate the need for passwords
- Verify identity data quickly and securely

The potential impact of decentralised and self-sovereign identity systems on society

The development of SSIs and decentralised identity management has the potential to change the relationships between government, companies, and individuals. In addition, the impact of SSIs on data storage in the digital world will need further and more stringent regulations when being assessed, as the technology enactment may result in no greater control or privacy afforded to the individual and may only reinforce current practices.

Strong regulation and a combination of centralised and decentralised governance may be required to avoid misuse of blockchains' less trackable features, such as the over-prevalence of users committing fraud or the trafficking of illegal substances and services.

With the oncoming introduction of the eIDAS 2.0 decentralised digital wallet, organisations, businesses, and regulatory bodies can better track fraud and illegal activities. Operating at the intersection of the public and private spheres, eIDAS 2.0 can provide the basis for solving many of the privacy, security and user experience problems experienced by European citizens in their digital lives.

By guaranteeing that the envisaged benefits of decentralised identity (as discussed in this article) are met and fully realised, eIDAS 2.0 could go a long way to ensuring that decentralised identity becomes a fundamental architectural component of tomorrow's internet.

The future of SSI

Self-sovereign identity (SSI) technology has the potential to significantly impact the future in various ways, transforming how individuals and organisations manage and interact with digital identities. Some of the key implications of SSI adoption include:

- **Enhanced privacy and control**: With SSI, individuals can manage their personal data and decide who gets access to it, which in turn enhances privacy and reduces the risk of data breaches or misuse.
- **Reduced reliance on centralised authorities**: SSI technology allows users to maintain and authenticate their digital identities without relying on a single, centralised authority, empowering the user to transparent and durable credentials.
- **Streamlined digital interactions**: By enabling the secure and efficient sharing of verifiable credentials, SSI can streamline various processes, such as opening a bank account, applying for a job, or accessing public services, making digital interactions more user-friendly and efficient.
- **Enhanced security**: The decentralised and cryptography-based nature of SSI systems makes them inherently more secure than traditional identity management systems, reducing the risk of identity theft, fraud, and data breaches.
- **Financial inclusion**: SSI technology can enable access to financial services and other essential services for underserved populations, particularly those without traditional identification documents, thereby promoting financial inclusion and social equity.
- **Interoperability and standardisation**: Widespread adoption of SSI could lead to increased standardisation and interoperability between different identity systems, making it easier for users to manage and share their digital identities across various platforms and services.
- **New business opportunities**: The adoption of SSI could create new business opportunities and revenue streams for companies providing identity-related

services, such as identity verification, data storage, and credential issuance.

- **Regulatory compliance**: SSI can help businesses and organisations more easily comply with data protection regulations, such as the General Data Protection Regulation (GDPR), by minimising the amount of personal data they need to store and process.

While these implications suggest a positive impact on the future, the widespread adoption of SSI depends on several factors, including the development of robust technical standards, the establishment of trust frameworks and governance models, and the willingness of individuals, organisations, and governments to embrace this new approach to digital identity management.

Current challenges and future directions:

The self-sovereign identity market is still in its infancy, with most yet to even hear about it, let alone figure out how to successfully deploy it at scale while also factoring in legacy issues, regulatory requirements and cost.

Despite this, there are a few companies, such as Truvity, that have already started down the long, arduous road of establishing decentralised identity protocols, developing and improving on the core technologies and providing a ready-to-order solution.

As discussed in this article, there are many practical benefits that businesses can achieve from adopting a decentralised identity. By working with a trusted provider with a strong reputation for successfully implementing SSI frameworks, businesses can begin shaping digital identity strategies that begin and end with their customer and ultimately, understand that what benefits the customer benefits the business.

The Truvity APK is your complete SSI solution

At its core, Truvity is a complex database solution that provides businesses with the data schemas, SSI mechanics, and modelling power to manage digital identities at scale. Securely manage and store user credentials through our easy-to-set-up wallet for seamless information exchange.

- **Personal Digital Wallet (PDW)**: Designed for creating, managing and storing product-defined personal wallets.
- **Enterprise Digital Wallet (EDW)**: Designed for creating, managing and storing corporate user wallets (candidate/employee).
- **Verifiable Credentials Apostille Office VCAO**: Delivers businesses the capacity to accept, review and verify paper documents scans and issue verifiable credentials.
- **Onboarding App**: Streamline compliance procedure; gather information with ease (create some digital twins in a case).
- **KYC Widget**: Seamless integration into all major CMSs for a 360° user experience.
- **Compliance Decision Panel CDP**: Compliance-specific environment to review documents, clarify issues, and make critical decisions. TBD

Use Truvity and unlock the full-power SSI. Prioritise trust through decentralised identity management with our cutting-edge, user-centric API platform.

Unlock a trustworthy internet with Truvity.

SIGN UP

Become an early adopter

Be one of the first to reap the benefits of Truvity

Sign up now

We're currently hiring. Learn more about us.

Sign up for email updates from Truvity

Your email address* SIGN UP

By subscribing I confirm that I have fully read and agree to the Truvity Terms and Conditions, including the Truvity Privacy Policy.

Email us hello@truvity.com

Platform Documentation Community Blog SSI Basics

Whitepaper About Careers eIDAS 2.0 Status

Terms and Conditions Cookie Policy Security Privacy Policy

© 2024 Truvity