Search Wikipedia

View history

Q

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute

Help
Learn to edit
Community portal
Recent changes
Upload file

Tools

What links here
Related changes
Special pages
Permanent link
Page information
Cite this page
Wikidata item

Print/export

Download as PDF
Printable version

Languages
Català
Deutsch
Español
Nederlands
Suomi
Українська
中文

Edit links

Self-sovereign identity

From Wikipedia, the free encyclopedia

Article Talk

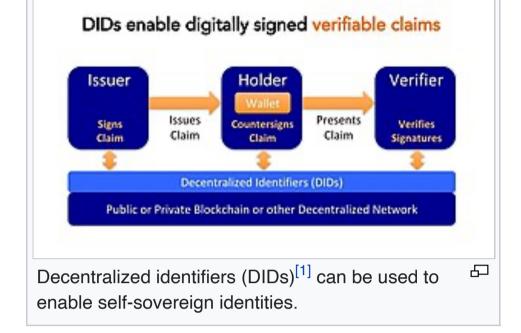


This article **provides insufficient context for those unfamiliar with the subject**. Please help improve the article by providing more context for the reader. (June 2020) (Learn how and when to remove this template message)

Self-sovereign identity (SSI) is an approach to digital identity that gives individuals control over the information they use to prove who they are to websites, services, and applications across the web. Without SSI, individuals with persistent accounts (identities) across the internet must rely on a number of large identity providers, such as Facebook (Facebook Connect) and Google (Google Sign-In), that have control of the information associated with their identity. [2] If a user chooses not to use a large identity provider, then they have to create new accounts with each service provider, which fragments their web experiences. Self-sovereign identity offers a way to avoid these two undesirable alternatives. In a self-sovereign identity system, the user accesses services in a streamlined and secure manner, while maintaining control over the information associated with their identity. [3] [4]

Contents [hide] 1 Background 2 Technical aspects 3 National digital identity systems 3.1 European Union 3.2 Korea 4 References

Relationship between entities, identities and attributes / identifiers



Background [edit]

5 See also

The TCP/IP protocol provides identifiers for machines, but not for the people and organisations operating the machines. This makes the network-level identifiers on the internet hard to trust and rely on for information and communication for a number of reasons: 1) hackers can easily change a computer's hardware or IP address, 2) services provide identifiers for the user, not the network. The absence of reliable identifiers is one of the primary sources of cybercrime, fraud, and threats to privacy on the internet.^[5]

With the advent of blockchain technology, a new model for decentralized identity emerged in 2015.^[6] The FIDO Alliance proposed an identity model that was no longer account-based, but identified people through direct, private, peer-to-peer connections secured by public/private key cryptography. Self-Sovereign Identity (SSI) summarises all components of the decentralized identity model: digital wallets, digital credentials, and digital connections.^[7]

Technical aspects [edit]

SSI addresses the difficulty of establishing trust in an interaction. In order to be trusted, one party in an interaction will present credentials to the other parties, and those relying parties can verify that the credentials came from an issuer that they trust. In this way, the verifier's trust in the issuer is transferred to the credential holder. This basic structure of SSI with three participants is sometimes called "the trust triangle".

It is generally recognized that for an identity system to be self-sovereign, users control the verifiable credentials that they hold and their consent is required to use those credentials.^[9] This reduces the unintended sharing of users' personal data. This is contrasted with the centralized identity paradigm where identity is provided by some outside entity.^[10]

In an SSI system, holders generate and control unique identifiers called decentralized identifiers. Most SSI systems are decentralized, where the credentials are managed using crypto wallets and verified using public-key cryptography anchored on a distributed ledger. The credentials may contain data from an issuer's database, a social media account, a history of transactions on an e-commerce site, or attestation from friends or colleagues.

National digital identity systems [edit]

European Union [edit]

The European Union is exploring decentralized digital identity through a number of initiatives including the International Association for Trusted Blockchain Application (INATBA) , the EU Blockchain Observatory & Forum and the European SSI Framework . The EU recently created an eIDAS compatible European Self-Sovereign Identity Framework (ESSIF). The ESSIF makes use of decentralized identifiers (DIDs) and the European Blockchain Services Infrastructure (EBSI). [12][13]

Korea [edit]

The Korean government created a public/private consortia specifically for decentralized identity.^[14]

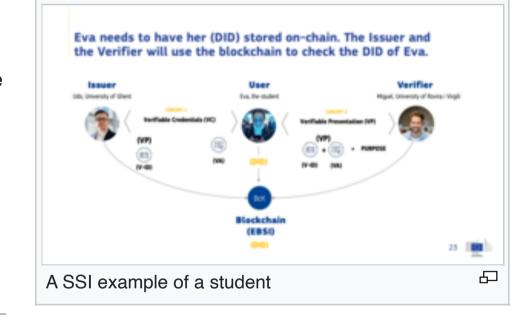
References [edit]

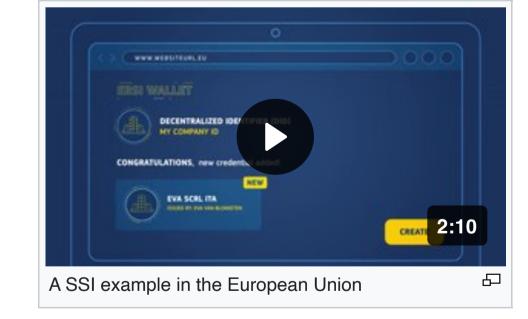
- 1. ^ "Decentralized Identifiers (DIDs)" ☑. World Wide Web Consortium. Retrieved 15 July 2020.
- 2. ^ Tobin, Andrew; Reed, Drummond. "The inevitable rise of self-sovereign identity" . The Sovrin Foundation.
- 3. ^ "Verifiable Claims Working Group Frequently Asked Questions" ☑. World Wide Web Consortium (W3C). 12 August 2022. Retrieved 12 August 2022.
- ^ Preukschat, Alexander (2021). Self-sovereign identity:
 decentralized digital identity and verifiable credentials .
 Drummond Reed, Christopher Allen, Fabian Vogelsteller, Doc Searls. Shelter Island, NY. ISBN 978-1-63835-102-3.
 OCLC 1275443730 .
- 6. ^ "History (2010-2014) Personal Data: Emergence of a New Assets Class" ☑. Decentralized Identity Web Directory. 2020-01-02. Retrieved 2022-08-12.
- 7. ^ a b Reed, Drummond; Preukschat, Alex (2021). Self-Sovereign Identity. Manning. p. Chapter 2. ISBN 9781617296598.

- 8. ^ Mühle, Alexander; Grüner, Andreas; Gayvoronskaya, Tatiana; Meinel, Christoph (2018). "A survey on essential components of a self-sovereign identity". *Computer Science Review.* **30** (1): 80–86. arXiv:1807.06346 ... doi:10.1016/j.cosrev.2018.10.002 ...
- Allen, Christopher (April 25, 2016). "The Path to Self-Sovereign Identity" ∠. Life With Alacrity. Retrieved
 February 19, 2021. "Users must control their identities....
 Users must agree to the use of their identity."
- 10. ^ "eIDAS supported self-sovereign identity" (PDF).European Commission. May 2019. Retrieved 16 June 2020.
- 11. ^ "Blockchain and digital identity" (PDF).
 eublockchainforum.eu. 2 May 2019. Retrieved 16 June 2020.
 12. ^ "Understanding the European Self-Sovereign Identity

European Commission. Retrieved 1 March 2021.

14. ^ 협회입니다, 한국디지털인증협회는 디지털신원증명의 진본성과 신뢰성을 확고히 하는 디지털 신원 인증 서비스를 위해 설립된 오픈 산업. "한국디지털인증협회" . 한국디지털인증협회 (in Korean). Retrieved 2022-08-12.





See also [edit]

- Decentralized identifier
- Decentralized web
- Digital self-determination

Categories: Authentication methods | Computer access control | Digital technology | Federated identity | Identity management | Sovereignty

This page was last edited on 18 November 2022, at 16:24 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License 3.0; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.