

Self-Sovereign Identity

What it is and what it is not

Frederico Schardong^{1,2}, Ricardo Custódio¹ (Supervisor)

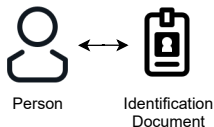
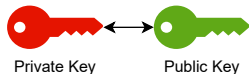
1 - LabSEC - Universidade Federal de Santa Catarina (UFSC)

2 - Instituto Federal do Rio Grande do Sul (IFRS)

April 27, 2022

Definition

Identity is commonly understood as a relation of **uniqueness** between two entities [1]



SSI History

- 1690 - John Locke's "The Second Treatise of Government"
 - "sovereignty resides in the people"
- 1859 - John S. Mill's "On Liberty"
 - "Over himself, over his body and mind, the individual is sovereign"
- 2012 - Devon Loffreto's blog post [2]
 - The first widely accepted [3–5] link between "sovereignty" and "digital identity"
- 2016 - Cristopher Allen's blog post "the path to self-sovereign identity" [3]
 - Ten principles of SSI

Allen's Ten Principles of SSI [3]

1. Existence: Users must have an independent existence (from the digital world)
2. Control: Users must control their identities
3. Access: Users must have access to their own data
4. Transparency: Systems and algorithms must be transparent
5. Persistence: Identities must be long-lived
6. Portability: Information and services about identity must be transportable
7. Interoperability: Identities should be as widely usable as possible
8. Consent: Users must agree to the use of their identity
9. Minimalization: Disclosure of claims must be minimized
10. Protection: The rights of users must be protected

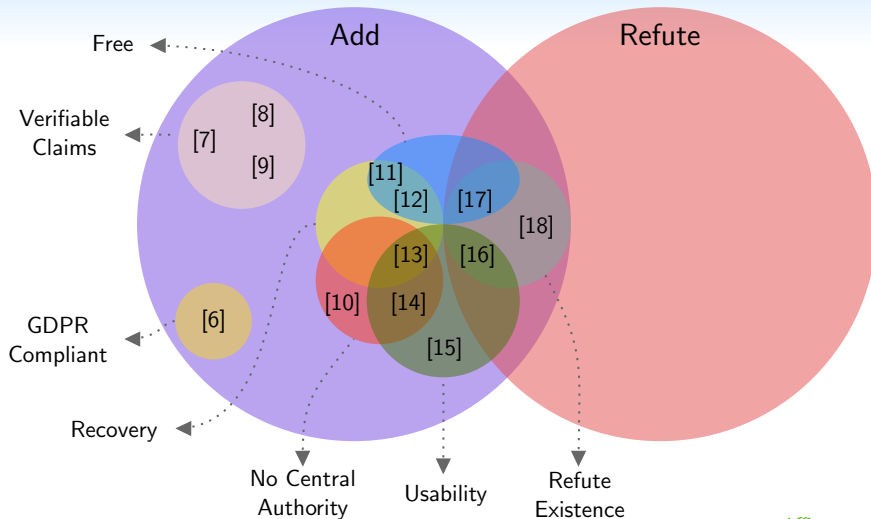


Figure: Source: [19]

What SSI is Not

“In essence it [SSI] is an identity management system which allows individuals to fully own and manage their digital identity.” [8]

- It is not a system.

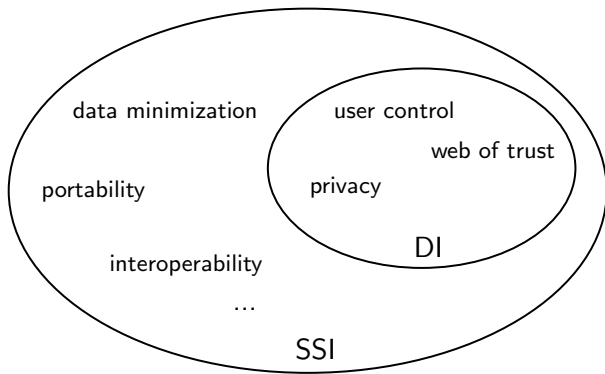
“The concept [SSI] is that one simply exists, therefore one has a digital identity. The identity is then built, managed and used by the owner of the identity.” [7]

- Only one identity?

What SSI is Not

- A system
- Identity + blockchain
- Anonymous credentials [20]
- W3C's DID and VC standards [21, 22]
- Decentralized Identity (DI)

SSI vs DI



DI

- Goal: eliminate authority
- Creation vs Control

SSI

- Goal:

What SSI is

An identity model ...

What SSI is

An identity model yet to be precisely defined

An identity model whose participants are autonomous

Readings

- In Search of Self-Sovereign Identity Leveraging Blockchain Technology [23]
- Schutte's Critique of the Self-Sovereign Identity Principles [18]
- A Critique of Immunity Passports and W3C Decentralized Identifiers [24]
- ...
- Self-Sovereign Identity: A Systematic Map and Review [19]

Questions?

Thank you for your attention.

frede.sch@gmail.com

References I

- [1] H. Noonan and B. Curtis, "Identity," in *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed., Summer 2018, Metaphysics Research Lab, Stanford University, 2018.
- [2] D. Loffreto, "What is "sovereign source authority"?" The Moxy Tongue. (2012), [Online]. Available: <https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html>.
- [3] C. Allen, "The path to self-sovereign identity," Life with Alacrity. (2016), [Online]. Available: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.
- [4] D. Searls, "Some perspective on self-sovereign identity," Kuppingercole. (2018), [Online]. Available: <https://www.kuppingercole.com/blog/guest/some-perspective-on-self-sovereign-identity>.
- [5] K. Young and Infominer, "Self-sovereign identity: Decentralized digital identity and verifiable credentials," in Shelter Island, ÛSA: Manning, 2021, vol. 1, ch. The origins of the SSI community, pp. 310–321, ISBN: 9781617296598. [Online]. Available: <https://livebook.manning.com/book/self-sovereign-identity/chapter-16/>.
- [6] M. Van Wingerde, "Blockchain-enabled Self-sovereign Identity," M.S. thesis, Tilburg University, 2017. DOI: 10.13140/RG.2.2.17693.82406.
- [7] Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada: IEEE, Jul. 2018, pp. 1336–1342. DOI: 10.1109/Cybermatics_2018.2018.00230.
- [8] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, Nov. 2018. DOI: 10.1016/j.cosrev.2018.10.002.
- [9] W3C Technology and society domain, "Verifiable Claims Working Group Frequently Asked Questions," World Wide Web Consortium (W3C). (2017), [Online]. Available: <https://w3c.github.io/webpayments-ig/VCTF/chapter/faq.html#self-sovereign>.
- [10] A. Abraham, "Self-sovereign identity: Whitepaper about the Concept of Self-Sovereign Identity including its Potential," 2017. [Online]. Available: <https://technology.a-sit.at/en/whitepaper-self-sovereign-identity/>.

References II

- [11] J. Andrieu, "A Technology-Free Definition of Self-Sovereign Identity," in *Rebooting the Web of Trust III*, San Francisco, USA: Web of Trust, 2016, pp. 2–5. [Online]. Available: <https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/topics-and-advance-readings/a-technology-free-definition-of-self-sovereign-identity.pdf>.
- [12] N. Naik and P. Jenkins, "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology," in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, Oxford, United Kingdom: IEEE, Aug. 2020, pp. 90–95. DOI: 10.1109/MobileCloud48802.2020.00021.
- [13] Z. Diebold and D. O'Mahony, "Self-Sovereign Identity using Smart Contracts on the Ethereum Blockchain," M.S. thesis, University of Dublin, 2017. [Online]. Available: <https://www.scss.tcd.ie/publications/theses/diss/2017/TCD-SCSS-DISSERTATION-2017-016.pdf>.
- [14] A. Satybaldy, M. Nowostawski, and J. Ellingsen, "Self-sovereign identity systems," in *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers*. Cham: Springer International Publishing, 2020, pp. 447–461, ISBN: 978-3-030-42504-3. DOI: 10.1007/978-3-030-42504-3_28. [Online]. Available: https://doi.org/10.1007/978-3-030-42504-3_28.
- [15] T. Speelman, "Self-Sovereign Identity: Proving Power over Legal Entities," M.S. thesis, Delft University of Technology, 2020. [Online]. Available: <https://repository.tudelft.nl/islandora/object/uuid:aab1f3ff-da54-47f7-8998-847cb78322c8>.
- [16] K. C. Toth and A. Anderson-Priddy, "Self-Sovereign Digital Identity: A Paradigm Shift for Identity," *IEEE Security and Privacy*, vol. 17, no. 3, pp. 17–27, May 2019. DOI: 10.1109/MSEC.2018.2888782.
- [17] J. Ellingsen, "Self-Sovereign Identity Systems Opportunities and challenges," M.S. thesis, Norwegian University of Science and Technology, 2019. [Online]. Available: <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617756>.
- [18] M. Schutte, *Schutte's Critique of the Self-Sovereign Identity Principles*, 2016. [Online]. Available: <http://matthewschutte.com/2016/10/25/schuttes-critique-of-the-self-sovereign-identity-principles/>.
- [19] F. Schardong and R. F. Custódio, "Self-sovereign identity: A systematic map and review," *CoRR*, vol. abs/2108.08338, 2021. [Online]. Available: <https://arxiv.org/abs/2108.08338>.

References III

- [20] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology — EUROCRYPT 2001*, B. Pfitzmann, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 93–118, ISBN: 978-3-540-44987-4. DOI: 10.1007/3-540-44987-6_7.
- [21] D. Reed, M. Sporny, D. Longley, A. Christopher, R. Grant, and M. Sabadello, "Decentralized Identifiers (DIDs)," World Wide Web Consortium (W3C). (2019), [Online]. Available: <https://www.w3.org/TR/did-core/>.
- [22] M. Sporny, D. Longley, and D. Chadwick, "Verifiable Credentials Data Model 1.0," World Wide Web Consortium (W3C). (2017), [Online]. Available: <https://www.w3.org/TR/vc-data-model/>.
- [23] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," *IEEE Access*, vol. 7, pp. 103 059–103 079, 2019. DOI: 10.1109/ACCESS.2019.2931173.
- [24] H. Halpin, "A critique of immunity passports and W3C decentralized identifiers," *CoRR*, vol. abs/2012.00136, 2020. arXiv: 2012.00136. [Online]. Available: <https://arxiv.org/abs/2012.00136>.