

Self-Sovereign Identity

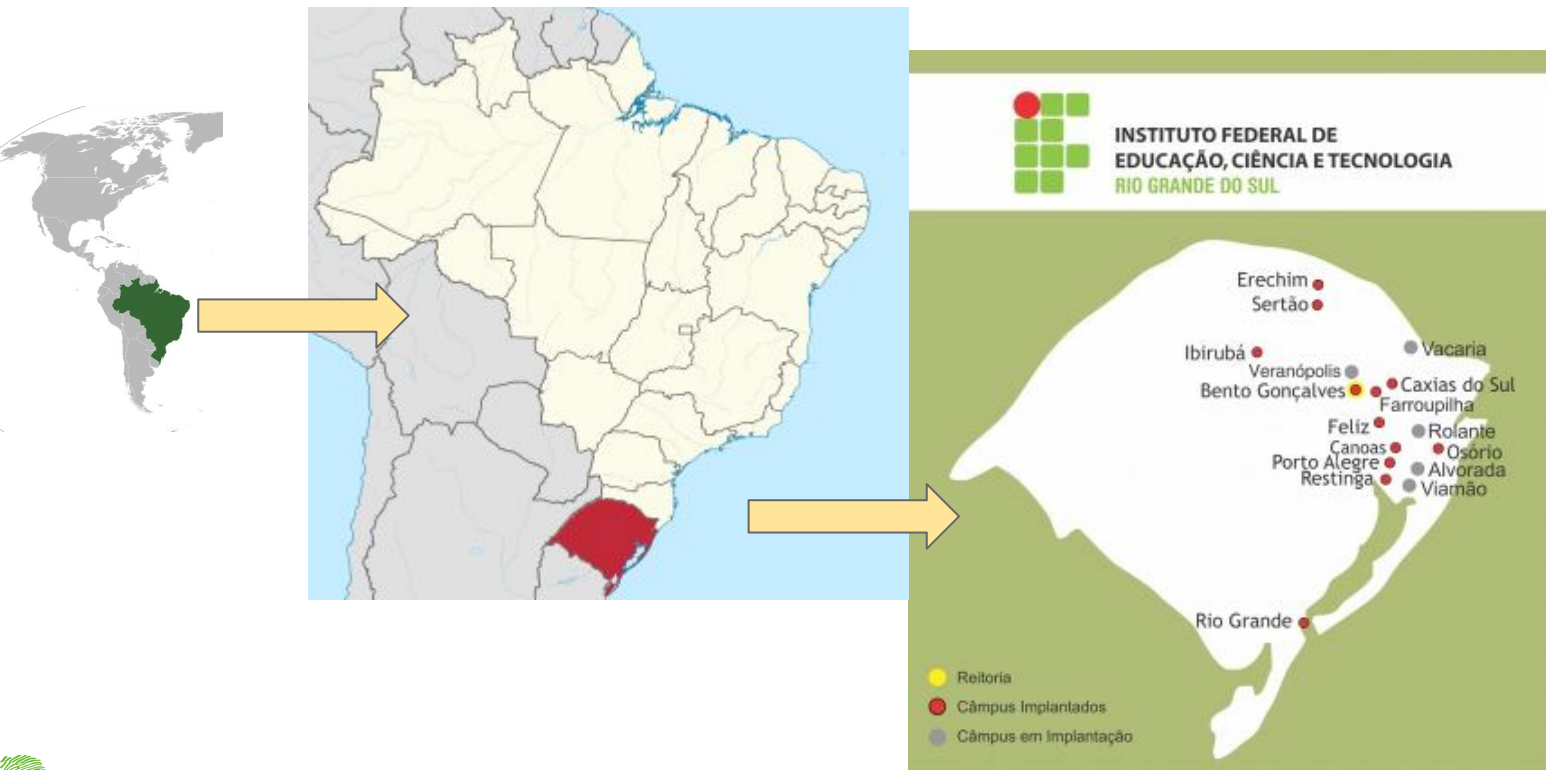
A New Paradigm for Identity Management and Its Open Challenges

Frederico Schardong

Laboratory of Computer Security (LabSEC)
Federal University of Santa Catarina (UFSC)
Federal Institute of Rio Grande do Sul (IFRS)

March 2023

Federal Institute of Rio Grande do Sul



22000 Students
1200 Professores
17 Campuses

What is identity?

What is identity?

“**Identity** is often said to be a relation each thing bears to itself and to no other thing” [1]

[1] H. Deutsch and P. Garbacz, “Relative Identity,” in The Stanford Encyclopedia of Philosophy, E. N. Zalta, Ed., Fall 2018, Metaphysics Research Lab, Stanford University.

What is identity?

“**Identity** is often said to be a relation each thing bears to itself and to no other thing” [1]

“To say that things are **identical** is to say that they are the same” [2]

[2] H. Noonan and B. Curtis, “Identity,” in The Stanford Encyclopedia of Philosophy, E. N. Zalta, Ed., Summer 2018, Metaphysics Research Lab, Stanford University

What is identity?

The indiscernibility of identicals* is usually formulated as follows [3]:

$$x = y \Rightarrow \forall F (Fx \Leftrightarrow Fy)$$

if x is **identical** to y, then x and y have all the same properties.

* Also called absolute identity, numerical identity, the standard account of identity or Leibniz Law

[3] P. Forrest, "The Identity of Indiscernibles," in The Stanford Encyclopedia of Philosophy, E. N. Zalta, Ed., Winter 2020, Metaphysics Research Lab, Stanford University.

What is digital identity?

What is digital identity?

“A digital identity is a **representation** of an entity in a specific context” [4]

[4] ISO, IT Security and Privacy - A framework for identity management
Part 1: Terminology and concepts, Standard, International
Organization for Standardization, Geneva, CH, March 2019.

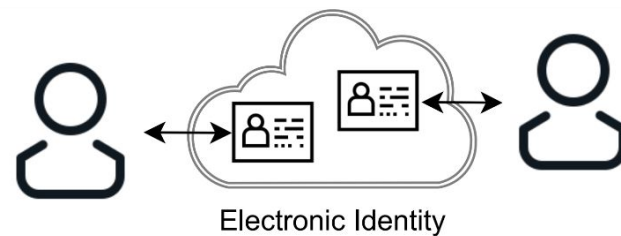
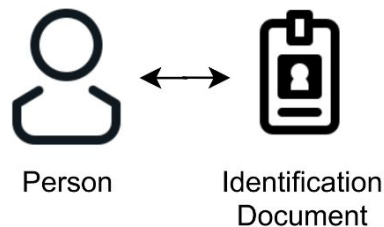
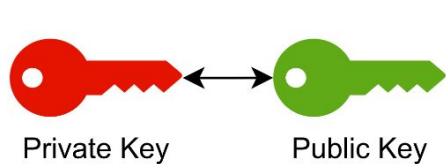
What is digital identity?

“A digital identity is a **representation** of an entity in a specific context” [4]

“A set of attributes **related** to an entity” [5]

What is identity?

Identity is a relation of **uniqueness** between two entities



Composition of a Digital Identity

Digital Identity

Identifiers

- Passport Number
- Email Address

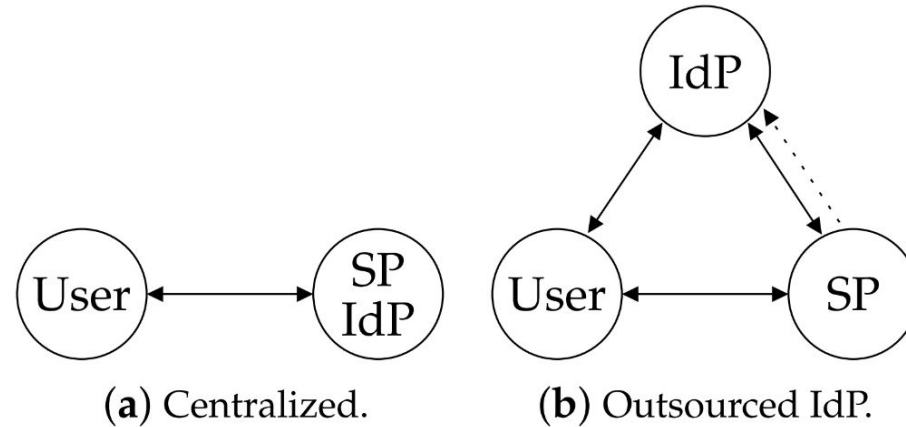
Access Credentials

- Password
- OTP

Other Attributes

- Cell Phone Number
- Name
- Birthdate
- ...

The Evolution of Digital Identity Models



[6] Schardong, Frederico, and Ricardo Custódio. "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy." *Sensors* 22.15 (2022): 5641.

Problems of Current Models

Problems of Current Models

Lack of freedom $\mapsto$ online existence should be independent of identity providers

Problems of Current Models

Lack of freedom $\mapsto$ online existence should be independent of identity providers

Lack of autonomy $\mapsto$ people need to be the controller of their attributes

Problems of Current Models

Lack of freedom $\mapsto$ online existence should be independent of identity providers

Lack of autonomy $\mapsto$ people need to be the controller of their attributes

Lack of privacy $\mapsto$ people's activity should not be monitored

Self-Sovereign Identity

Self-Sovereign Identity (SSI) [7] is an digital identity model, where:

- People manage their personal information (credentials);
- Credential presentation minimizes information leakage;
- IdPs are not aware of how credentials are used.

[7] Allen, C. The Path to Self-Sovereign Identity. 2016. Available online:
<http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>

Self-Sovereign Identity

There is no precise definition of self-sovereign identity (SSI) [6]

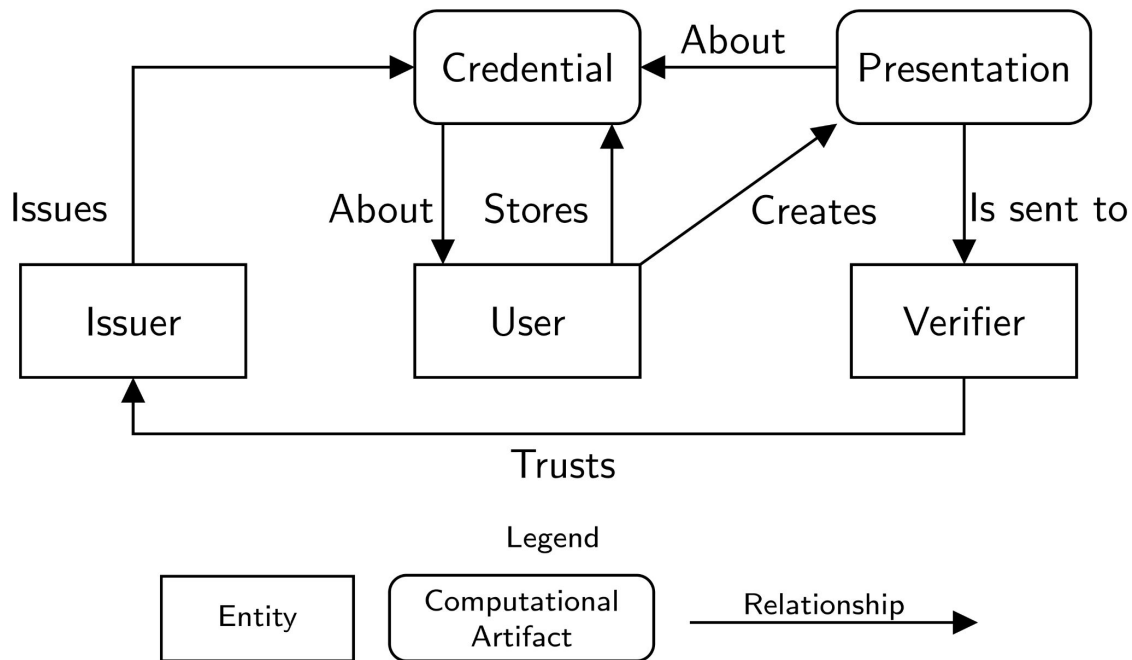
- [6] Schardong, Frederico, and Ricardo Custódio. "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy." *Sensors* 22.15 (2022): 5641.

Table 7: Publications that add or refute philosophical views of SSI.

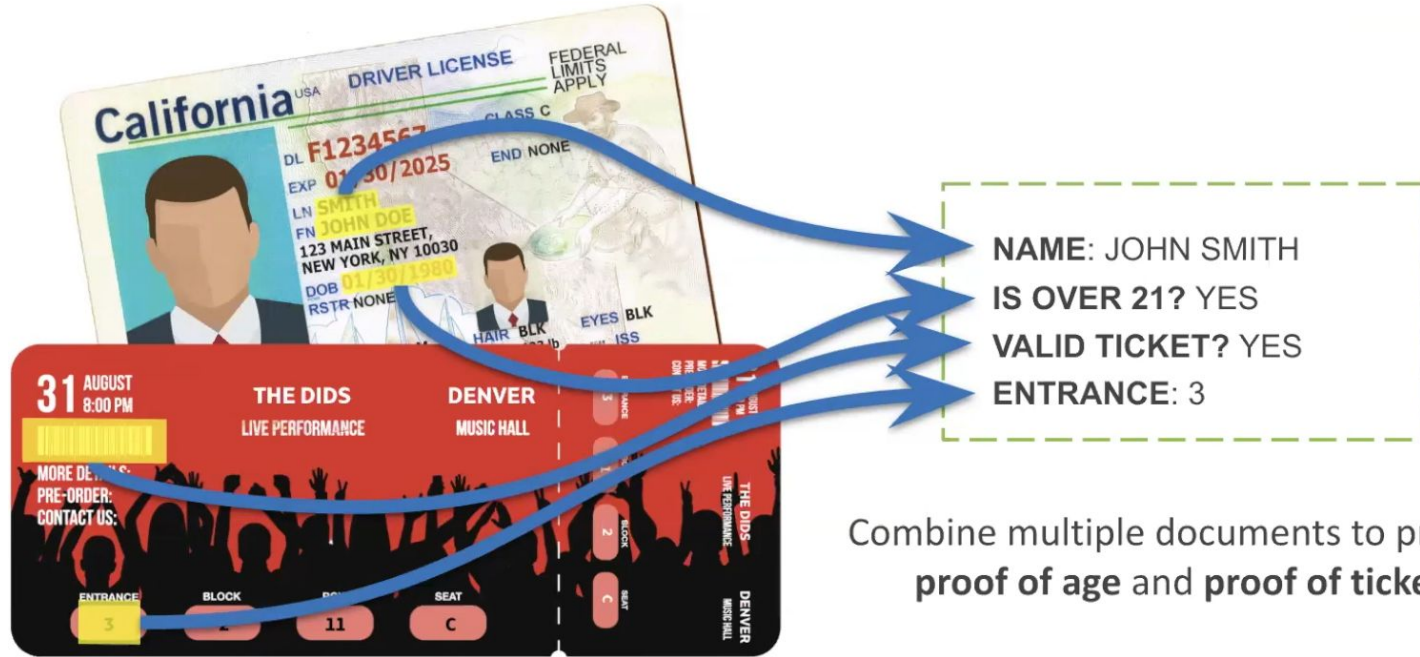
Works	Add														Refute								
	Functional							Non-Functional															
	No Central Authority	Legacy Compatible	Verifiable Presentation	Counterfeit Prevention	Identity Verification	Identity Assurance	Secure transactions	Delegation	Recoverability	Usability	Accessibility	Availability	Auditability	Scalability	Free	Regulatory	Existence	Control	Access	Consent	Persistence	Transparency	Protection
[19, 112, 197]			✓																				
[198]	✓	✓	✓						✓					✓	✓								
[199]			✓				✓		✓		✓			✓	✓								
[128]												✓											
[200]															✓		✓						
[201]			✓						✓							✓							
[202]	✓																						
[203]	✓									✓				✓									
[204]	✓								✓	✓													
[205]										✓													
[59]				✓	✓	✓	✓			✓							✓					✓	✓
[116]			✓													✓							
[206]	✓	✓				✓	✓		✓	✓	✓												
[207]	✓		✓				✓	✓		✓	✓												
[208]													✓				✓	✓	✓	✓	✓		

[6] Schardong, Frederico, and Ricardo Custódio. "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy." *Sensors* 22.15 (2022): 5641.

Self-Sovereign Identity



Self-Sovereign Identity



Combine multiple documents to present
proof of age and **proof of ticket**.

SSI: Common Misconceptions

SSI: Common Misconceptions

- Technically something new, see [8]

SSI: Common Misconceptions

- Technically something new, see [8]
- Requires blockchain, see [6]

[6] Schardong, Frederico, and Ricardo Custódio. "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy." *Sensors* 22.15 (2022): 5641.

SSI: Common Misconceptions

- Technically something new, see [8]
- Requires blockchain, see [6]
- Requires W3C's DID and VC standards

SSI: Open Challenges

SSI: Open Challenges

- A definition of SSI that researchers and practitioners accept

SSI: Open Challenges

- A definition of SSI that researchers and practitioners accept
- Fundamental research

SSI: Open Challenges

- A definition of SSI that researchers and practitioners accept
- Fundamental research
- Special case attribute sharing

SSI: Open Challenges

- A definition of SSI that researchers and practitioners accept
- Fundamental research
- Special case attribute sharing
- Sound trust models

SSI: Open Challenges

- A definition of SSI that researchers and practitioners accept
- Fundamental research
- Special case attribute sharing
- Sound trust models
- Blockchainless SSI

SSI: Open Challenges

- A definition of SSI that researchers and practitioners accept
- Fundamental research
- Special case attribute sharing
- Sound trust models
- Blockchainless SSI
- To facilitate the migration from other paradigms

SSI: Open Challenges

- A definition of SSI that researchers and practitioners accept
- Fundamental research
- Special case attribute sharing
- Sound trust models
- Blockchainless SSI
- To facilitate the migration from other paradigms
- Usability

Thank you!

Contact me



frede.sch@gmail.com