Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

DELFI 2021 Workshop

A User-Model for a Next Generation Learning Management System

Self-Sovereign Identities (SSI)

From vision to today

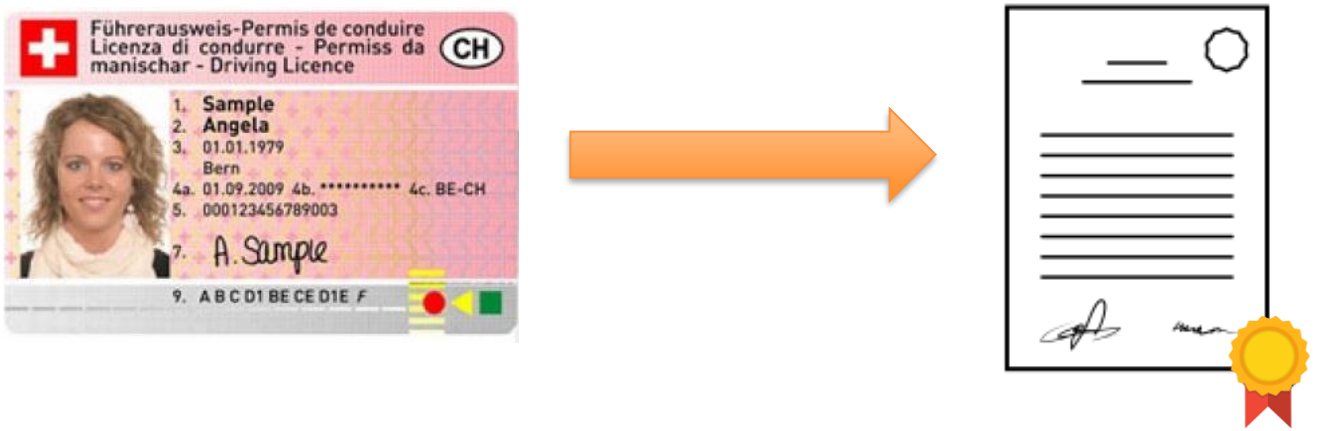
Prof. Dr. Annett Laube-Rosenpflanzer, BFH, Institute IDAS

Goals

- Introduction to SSI
- Decentral, user centric identities
- A little bit of history
- Advantages & Challenges
- Picture #5

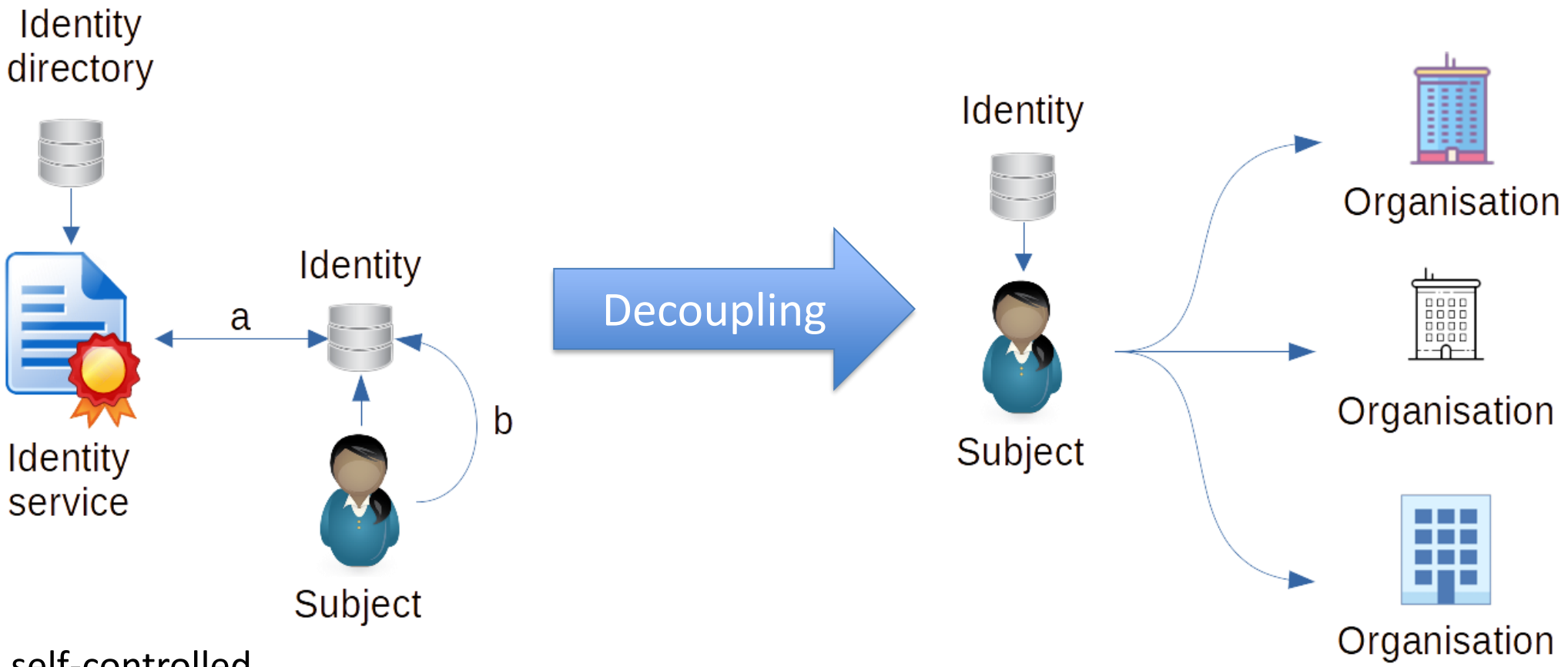
Self-Sovereign Identities (SSI)

- Digital counterpart to ID documents



- The user is the owner (and administrator) of their electronic identity and thus in possession of their personal data.
- There is no central storage of identity data.
- The issuer does not know where and when the identity is used.

Decentral, user centric approach

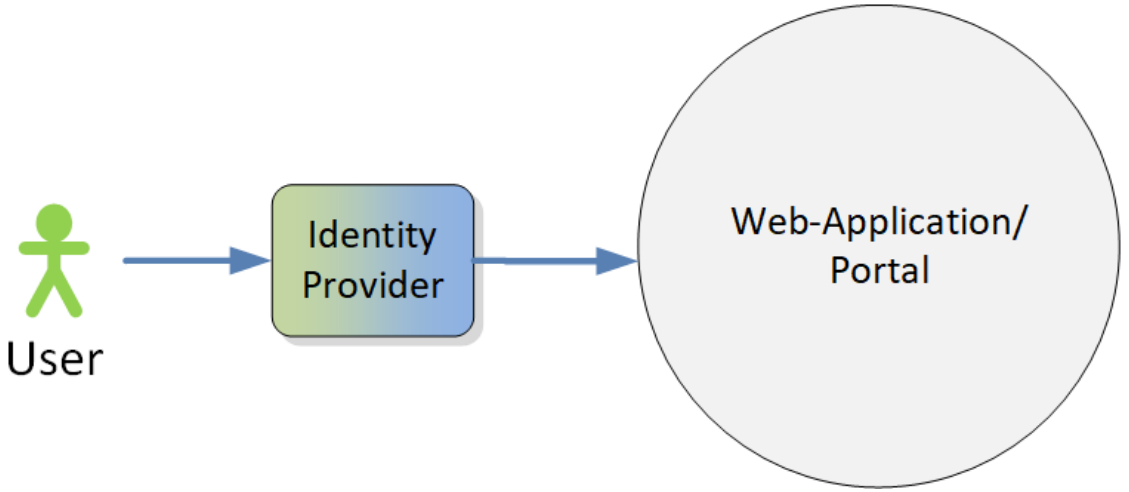


(a) self-controlled

(b) self-managed (self-sovereign)

Today's Identity Federation

- The identity provider is always involved
  - All personal information is passed through
  - Privacy could be an issue
- User must trust the identity provider
- User is dependent on the identity provider



The vision

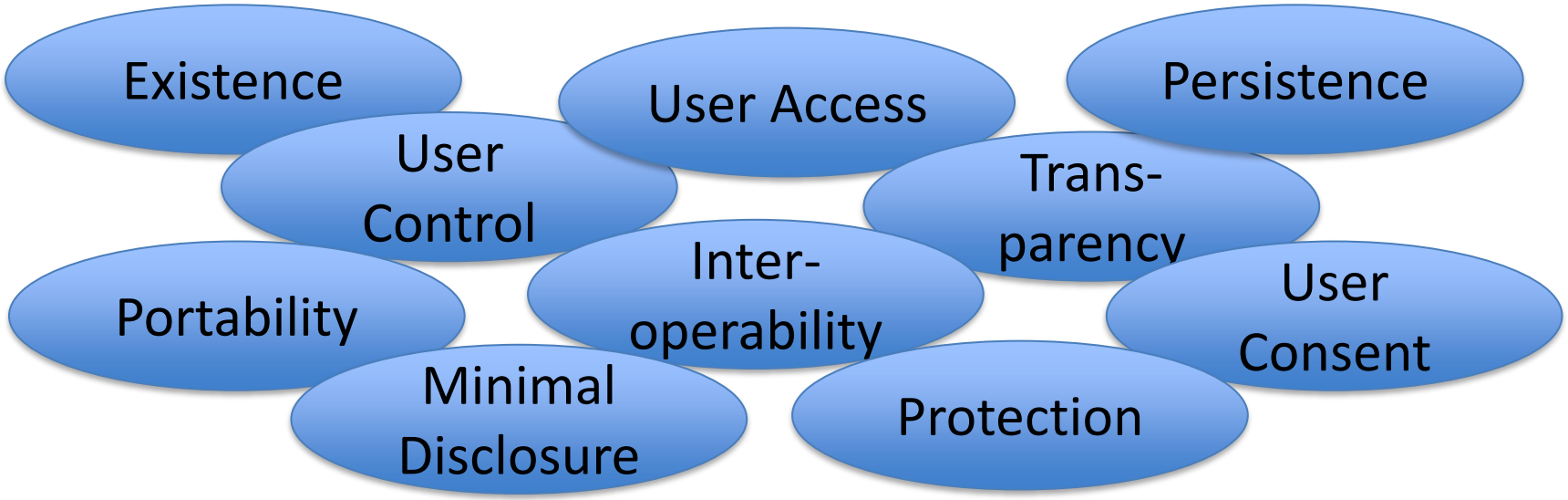
'Self-Sovereign Identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity.'

— Christopher Allen

The SSI Vision

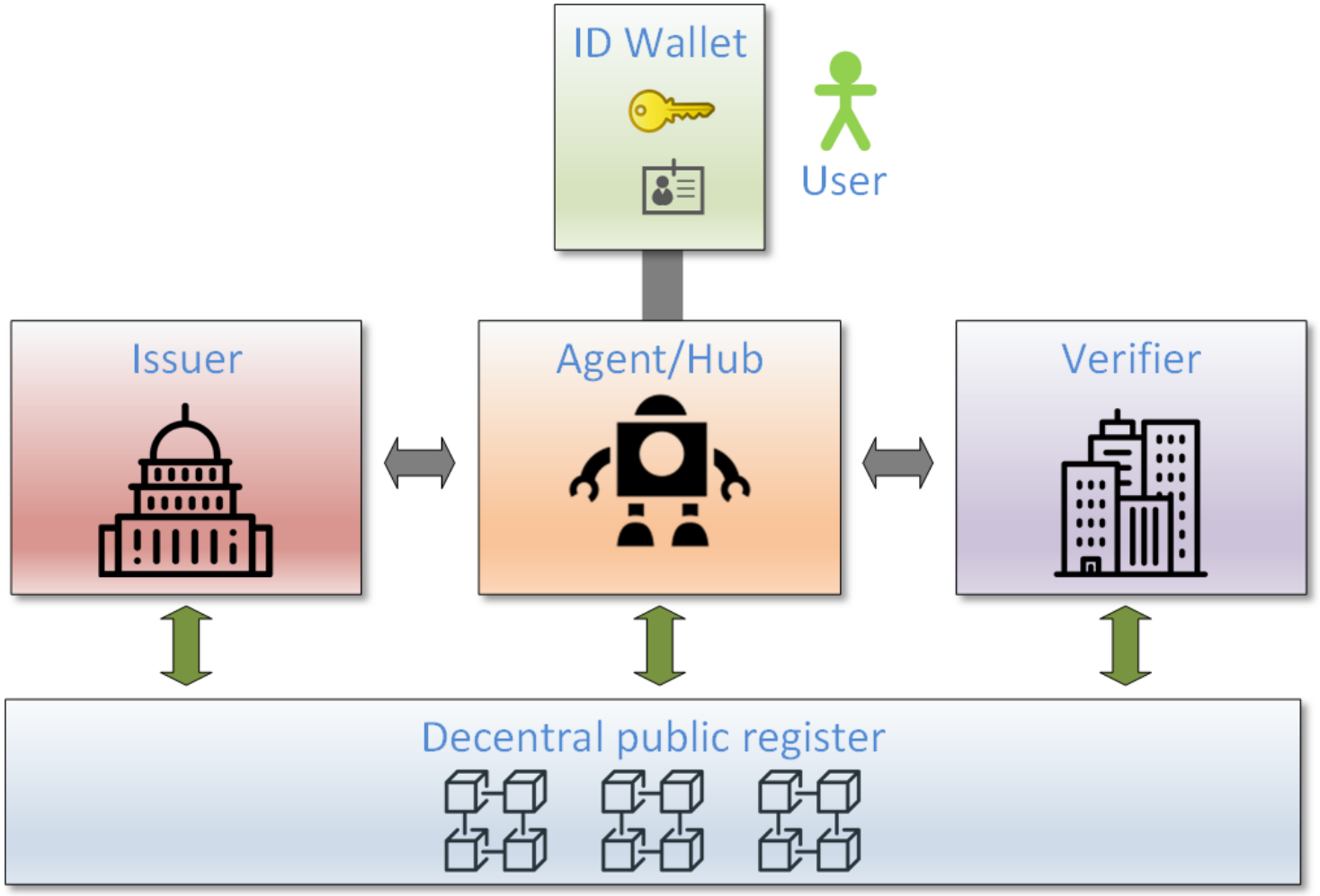
Goals:

- digital identities that are **trustworthy** and at the same time **protect the privacy** of the individual
- an identity system that balances transparency, fairness, community support and individual protection.

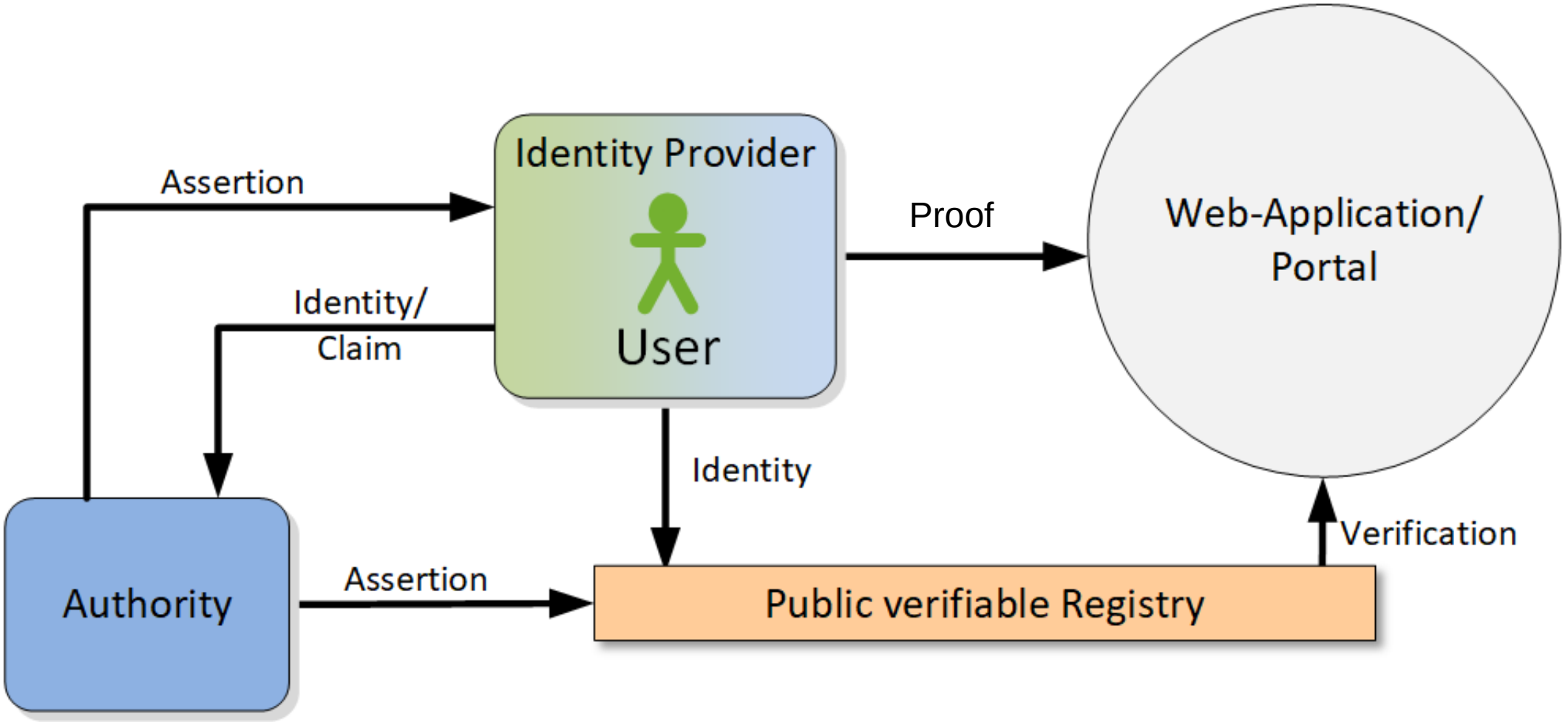


The 10 Principles from Ch. Allen 2017

SSI main components



Decentral Identity



Challenges of SSI

Is a normal user ready for this?

- High complexity
- No support in case of problems
  - E.g., when private keys are lost
- User is in charge for backup, synchronization between different devices, …
- Establishment of trust
- Governance
- Implementation effort/cost ?

- **Privacy not by default**
  - If one identity is used for all -> tracking/profiling possible
  - Use of multiple identities or zero-knowledge proofs required

Principles for SSI ecosystems

- Published in Dec. 2020: https://sovrin.org/principles-of-ssi/

- **Goals:**
  - Better usability
  - Less complexity for the user
  - Easy access for normal users.

- **Realization:**
  - Restriction of **one ecosystem:** Not one identity for all, but one for an ecosystem (e.g., academia, public transport, health)
  - The identity and its verified attributes are **issued by the identity service** of the ecosystem and given to the user -> **self-controlled identities**
  - **Agents and gateways** support the user.

Advantage and disadvantages of SSI ecosystems

- Usability and easy access (complexity is hidden).
- Central governance
- Clear trust relations
- No public blockchain required (ecological advantage)

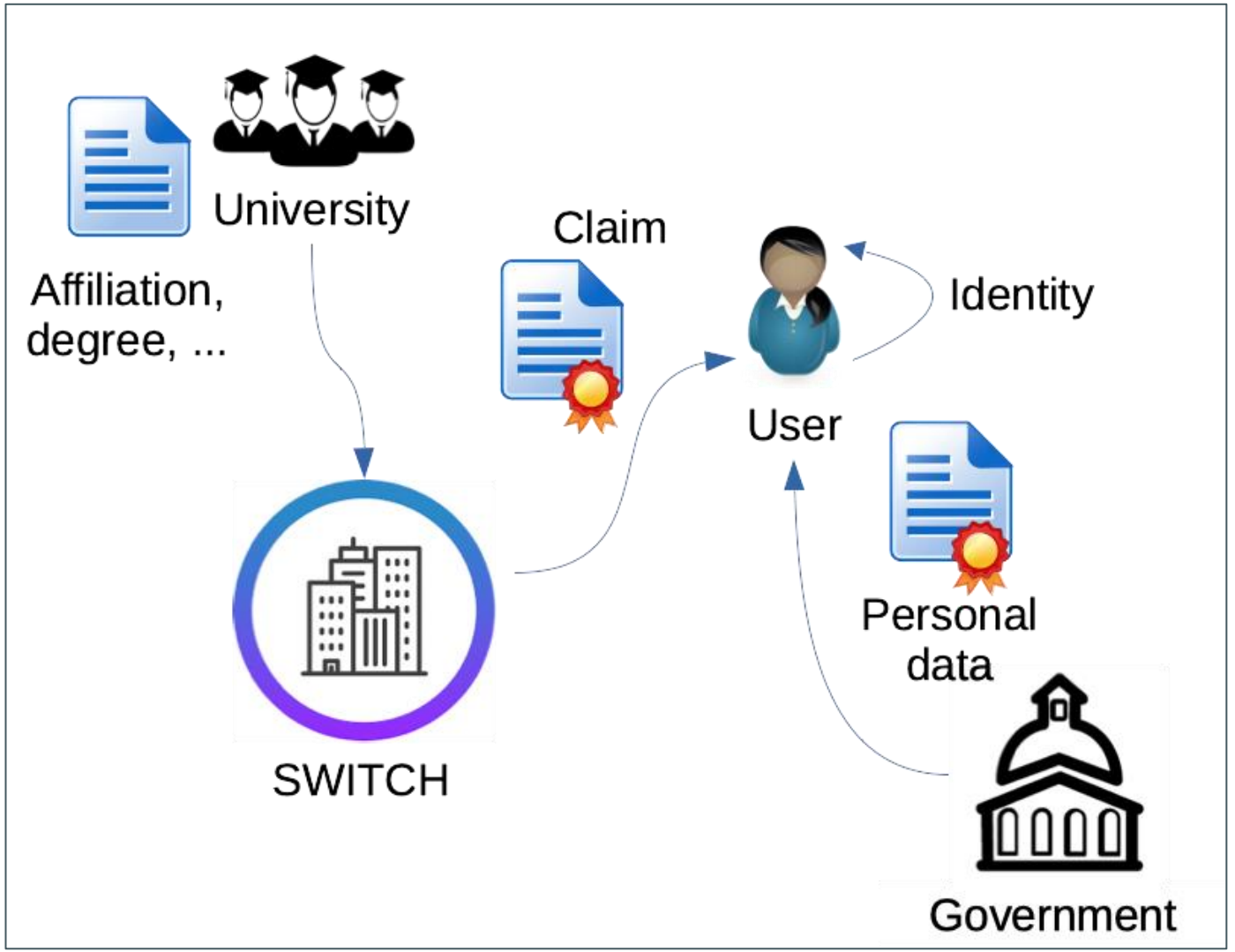
- Existing trust, based on contacts or relationships, can be extended to the SSI ecosystem

- User **must trust** the ecosystem, esp. the agents and gateways
  - All personal information passes through
  - Privacy and data protection not guaranteed

- Interoperability between ecosystems
- Transparency?
  - Open source?
  - Disclosure of algorithms?

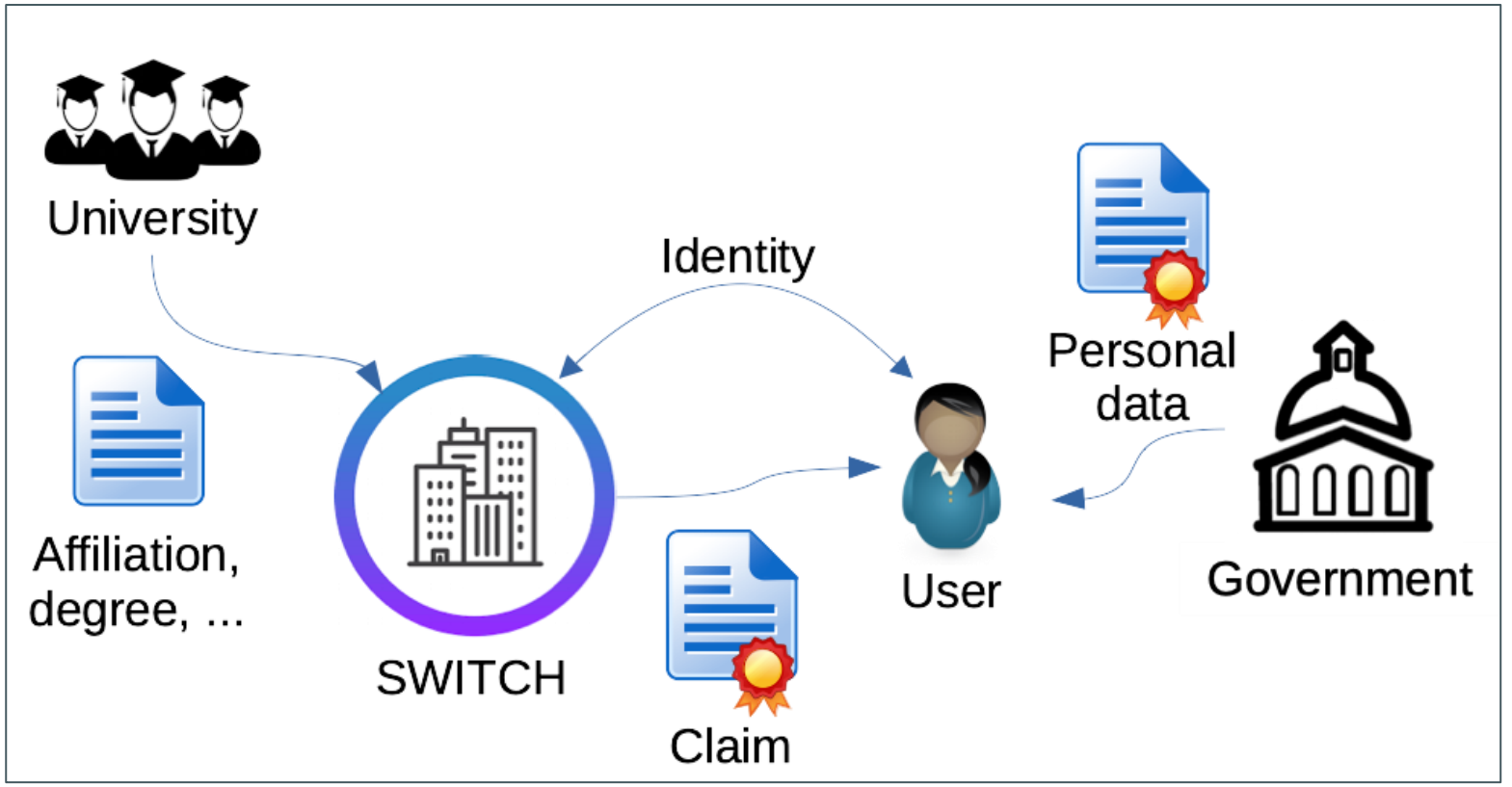
Picture #5a: Self-Controlled Identities

- Users create their own identity.
- “Personal data” is issued by a governmental authority (based on users’ self-issued Identity).
- SWITCH issues users’ claims on behalf of the universities (based on the self-issued Identity of the user).



Picture #5b: SWITCH SSI ecosystem

- SWITCH creates a bootstrap identity in agreement with the user.
- This identity is maintained locally (at the users' device) and centrally by SWITCH. Personal data is issued by a governmental authority.
- SWITCH issues users' claims on behalf of the universities.
- The user can now present its verifiable credentials to any RP without issuer.



Thank you !! Any Questions?

Contact: annett.laube@bfh.ch

Quellen

- https://freecontent.manning.com/the-basic-building-blocks-of-ssi/
- https://trinsic.id/what-is-self-sovereign-identity/
- https://www.societybyte.swiss/2020/02/12/self-sovereign-identities-kontrollieren-wir-in-zukunft-unsere-identitaet-selbst/
- https://www.societybyte.swiss/2020/02/06/es-braucht-sichere-identitaeten-fuer-das-vertrauen-der-kunden/