HSLU Hochschule Luzern

Who am I:

Online identification and verification considering new developments such as Web3 and Distributed Ledger Technology

Hochschule Luzern
Informatik

Ursula Sury
Vizedirektorin
T direkt +41 41 757 68 52
ursula.sury@hslu.ch

13.06.2023

FHZ Zentralschweiz

HSLU Hochschule Luzern

TABLE OF CONTENT

Self Sovereign Identity

HSLU Hochschule Luzern

CASE 1

You are applying for a job at Y. AG:

You keep your diplomas and previous work experience in your e-wallet, as part of your Self-Sovereign Identity.

- How does it work in today's world?
- What would be possible with Self Sovereign Identity?

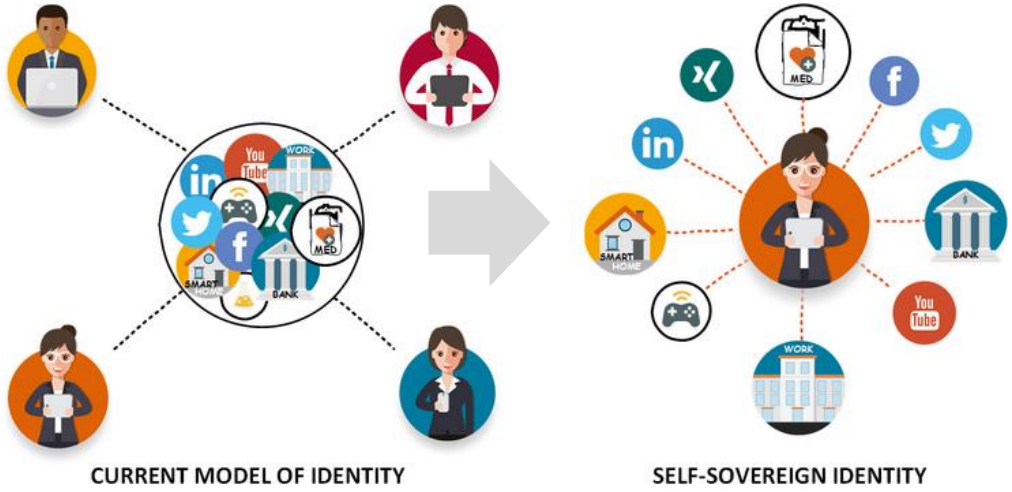
CASE 2

Your son has just turned 16 and wants to buy his first bottle of wine himself to celebrate the occasion. He orders it from the Haddock GmbH shop. The latter wants a valid proof of his age. He also has an e-ID and an e-wallet.

- How are things today?
- How is it different with the E-ID?

HSLU Hochschule Luzern

SELF SOVEREIGN IDENTITY



Bildquelle: https://hpi.de/meinel/lehre/master-projects/self-sovereign-identity-with-blockchain-technology.html

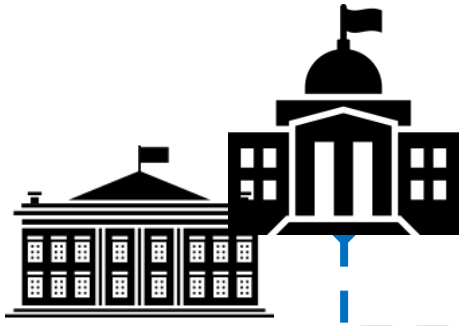
- The self-determined identity or **Self-Sovereign Identity (SSI)** brings the identity back to the user.
- It works similarly to the physical identity. The user keeps the identity data with him (analogous to the ID in a **wallet**).
- It works similarly to the physical identity. The user keeps the identity data with him.
- SSI solves the **missing identity functionality** of the internet or digital media in general.
- At the same time, **independence** from a central issuing and managing entity is guaranteed.
- The data remains with the user (important for data protection). **Blockchain** can be used as a storage for credentials but does not have to be used.

HSLU Hochschule Luzern

Holder

Third parties (Verifier)

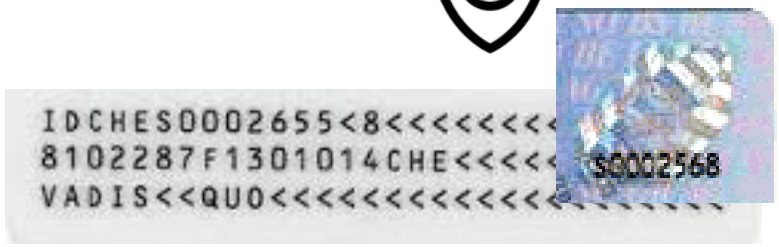
Issuer



Confederation, Universities, Banks, …

Trust

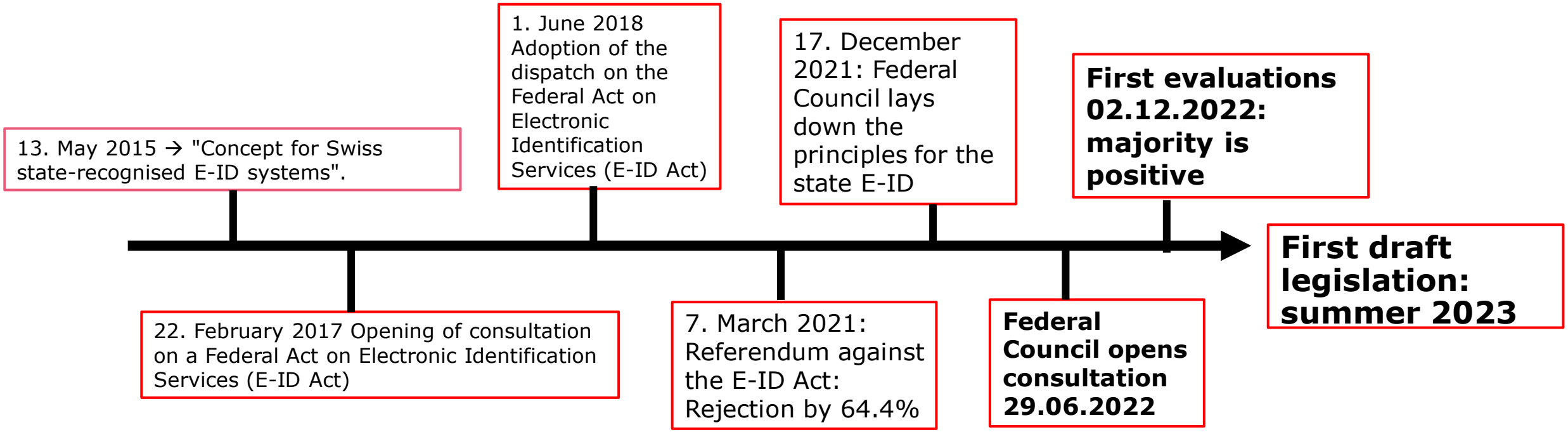
Trust anchor



No direct link

HSLU Hochschule Luzern

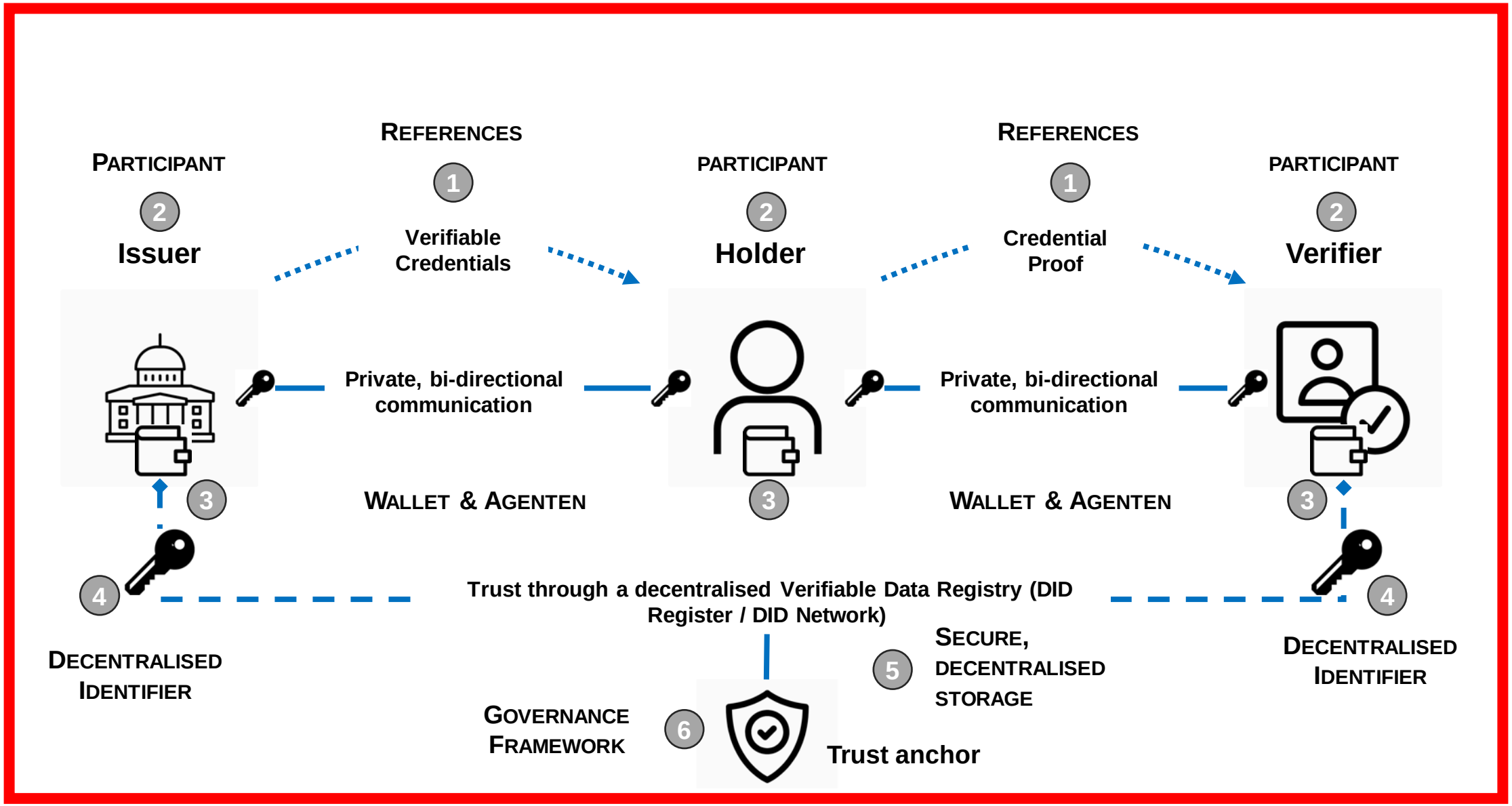
E-ID – HISTORY



Public law

Data protection

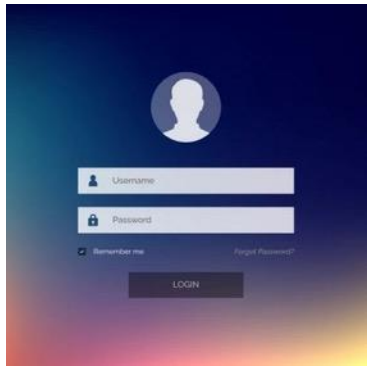
Civil law



HSLU

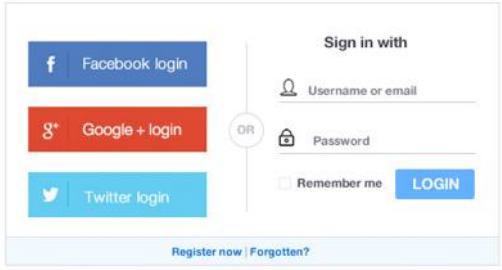
Accountability and organisation

«Silo»-System



Self Sovereign Identity

physical proof of identity



Intermediary

HSLU Hochschule Luzern

Role of the federation

Role of technology

«Human Trust»

- Legitimised trust framework
- Commonly defined and lived rules
- Accepted quality requirements
- Certified processes and technologies

«Crypto Trust»

- Cryptographic methods
- Decentralised, consensus-based system technologies
- Bidirectional, multi-device capable protocols
- Open source and internationally recognised specifications

SUMMARY

- **Self-Sovereign Identity (SSI) covers the various stakeholder and policy requirements for E-ID.**
- SSI enables the passport/ID to be brought into the digital world as one building block of a growing ecosystem.
- SSI is **independent of an issuing party** and can be used for different identity proofs (e.g. personal data, credentials, access authorisation).
- SSI is **more than a technology** and encompasses many other topics (e.g. legal foundations, governance, data protection).
- **Blockchain** can be used as a trust anchor, but it does not have to be. However, a decentralised and trustworthy infrastructure is important.
- International compatibility with other countries can be ensured through **compliance** with standards (e.g. W3C - DID).

Who Am I?

An Important Comprehension of Self Sovereign Identity

DELIMITATIONS

Self Sovereign Identity is NOT:

- Passport or Identity Card
- Verification
- Digital Signature
- Fulfilment of a contractual formal requirement

	Identification	Verification
Definition	Detection features are compared with **several or all** references stored in the system	Detection features are compared with **only one** reference stored in the system
example	The passport; identity card - E-ID based on it	Entering a PIN
Explication	An identification is a process that enables a person to be uniquely recognised.	In the case of verification, it is sufficient to enter a certain combination of numbers, for example. So you only have to prove that the specified requirements (in our case the combination of numbers) are met.

Digital signature and forms of contract

DIGITAL SIGNATURE AND FORMS OF CONTRACT

Forms of contract in general	Digital signature
Principle: No formal requirement, Art. 11 CO **Exception:** 1. Legally prescribed written form (Art. 12 ff. CO). 2. Contractually prescribed written form (Art. 16 CO) 3. Public certifications	**Art. 14 Abs. 2bis Code of Obligations** *2bis An authenticated electronic signature combined with an authenticated time stamp within the meaning of the Federal Act of 18 March 2016 on Electronic Signatures is deemed equivalent to a handwritten signature, subject to any statutory or contractual provision to the contrary* = **Federal Act of 18 March 2016 on Electronic Signatures**

Data Protection

WHAT IS DATA PROTECTION?

Data Protection = Protection of Personality

Consent

Legal Foundation

Purpose

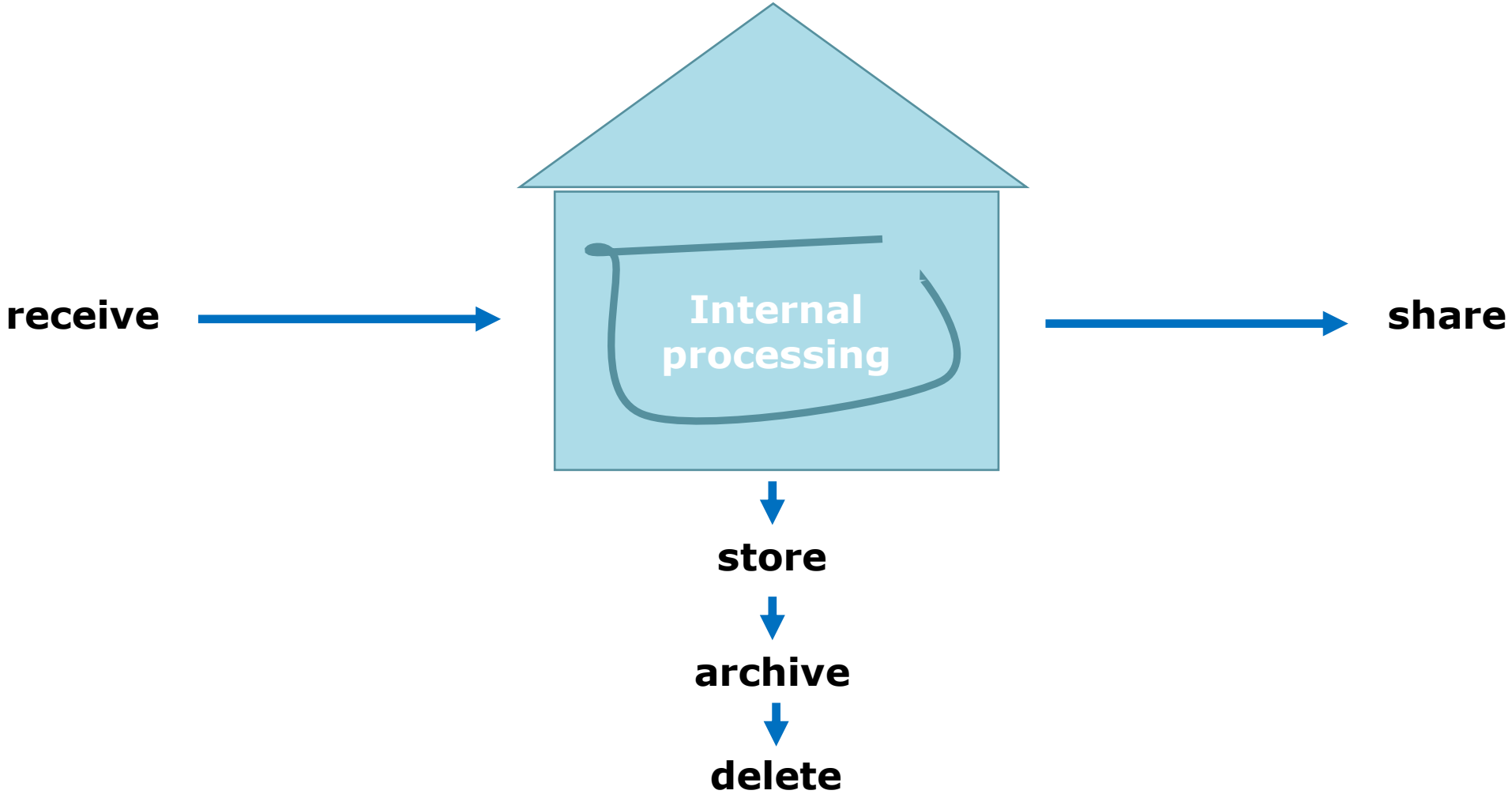
↑

Proportionality
Accuracy
Security

- Privacy by Design
- Privacy by Default

Processing = any handling of data

WHAT IS MEANT BY DATA PROCESSING?



OVERVIEW OF SANCTIONS IN DATA PROTECTION LAW

	Who?	Why?	Sanction
Sanctions EU	• **companies**	**Sanctions pursuant to Art. 83 GDPR:** For formal or material breaches of Art. 5-58 GDPR: • Failure to comply with **privacy by default** (Art. 25 GDPR). • Failure to fulfil the duties of the **data protection officer** (Art. 39 GDPR) • Breach of the principles relating to the **processing of personal data** (Art. 5 GDPR) • Violation of the **rights** of the data subjects	• **Fines of up to EUR 20,000,000 or 4% of the company's worldwide annual turnover**. • For less serious infringements, up to **EUR 10,000,000 or 2% of the company's worldwide annual turnover** (Art. 83 GDPR).
Sanctions Switzerland as of september	• **Private individuals**	**A fine is imposed on private individuals on request if they provide false or incomplete information:** • Violation of duties under Art. 19, 21 and 25- 27 nDSG. • Violation of the duty to provide information • Violation of due diligence obligations	• **Fines of up to CHF 250,000** • offences in business establishments**, fine up to CHF 50,000**

HSLU Hochschule Luzern

DATA PROTECTION AS A COMPANY ASSET

data protection impact assessments

Certifications: Art. 13 nDSG

Processing directories: Art. 12 nDSG

Codes of Conduct: Art. 11 nDSG

Appointment of a data protection officer

+

Governance on a data protection level

=

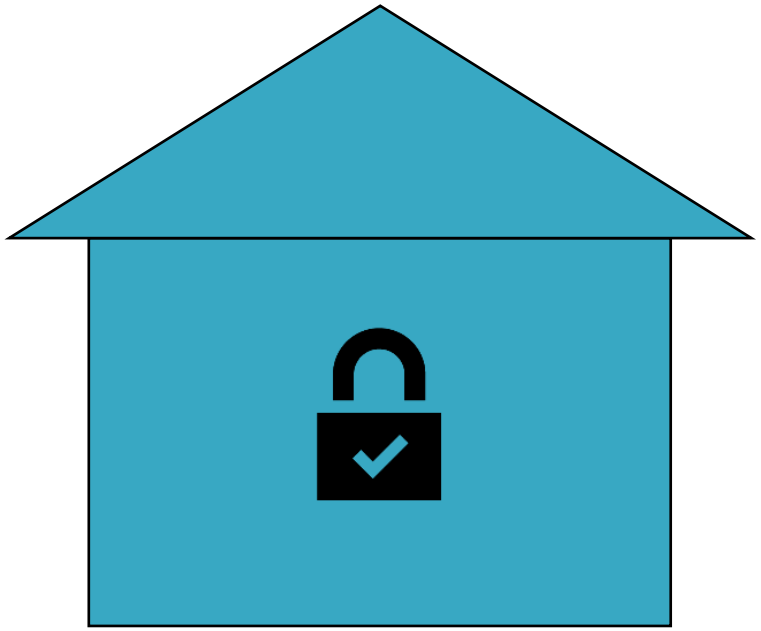
Overview and control of data processing within the company; external and internal security

From Cost to Asset!

SSI and Data Protection

PRINCIPLES OF DATA PROTECTION

- **Privacy by Design**
  Privacy Impact Assessment (PIA)Privacy by Technology:
  Data controllers are obliged to take appropriate technical measures.
- Examples:
  - Adaptation of software
  - Adaptation of the organization
- **Privacy by Default**
  Products must be set to be data protection-friendly by default.
- Examples:
  - Browser blocks cookies with installation requests.
  - Social media account is set to "non-public" by default.



THE ROLE OF DATA PROTECTION

Personal data must be protected

- Privacy by design
- User must have data sovereignty
- Minimal data disclosure = Use of Zero-Knowledge-Proof (ZKP) "Nobody needs to know the date of birth for an age check".

Maximum possible data security

- No single point of failure
  - Decentralised solution
- Flexibility for data security adjustments

Governance

Issuer

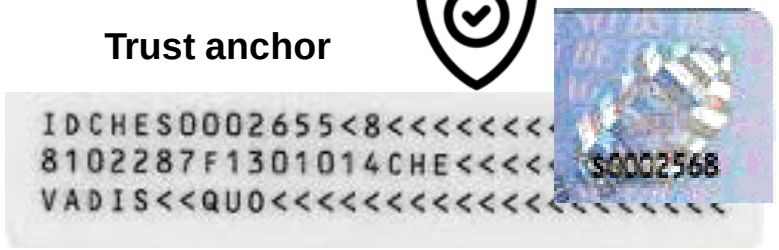
Confederation,
Universities,
Banks, …

Holder

Third parties
(Verifier)

Trust

Trust anchor



No direct link

HSLU Hochschule Luzern

WHAT ARE THE KEY DRIVERS IN THE SHIFT TO THE NEXT WEB?

- Trust/ Anchor of Trust -> Who?
- Standardisation in CH and Europe
- Privacy by Design/ Privacy by Default (Metadata)
- Interdisciplinarity
- Digital Ecosysteme → Physical World
- User friendliness

ADVANTAGES AND DISADVANTAGES

- Everyone is master of their own data; Self **Sovereign I**dentity
  - Sovereignty over the sharing and processing of one's own e-wallets
- Clear overview of one's own data
  - Both private and corporate; SSI as an asset
- Better implementation of Privacy by Design and Data Protection principles
  - SSI protects the user better; no unwanted relinquishment of control over one's own data
  - Principle of data economy and proportionality of data processing
  - Only as much data needs to be shared as necessary

- What happens to the data shared with the Verifier?
  - The principles of data protection law all still apply!
- How to establish trust between the Issuer and the Verifier?

Digital for a better World

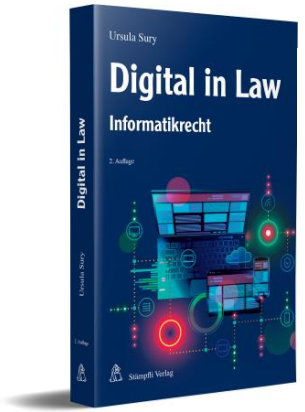
HSLU Hochschule Luzern

SECURE FORMS OF COMMUNICATIONS

	Regular letter	Registered letter	Regular email	Encrypted Email	Signed Email	Registered email
Undeniability of receipt		x				x
Undeniability of the sender					x	x
Trustworthiness	(x)	x		x		x
Integrity	x	x			x	x
Fast delivery			x	x	x	x
Content can be proven					x	x

Any questions?

Publikationen der Referentin



› Gibt einen umfassenden Überblick über die Rechtsaspekte in der digitalen Welt

Digital in Law, Informatikrecht, Stämpfli Verlag 2021

Diverse Beiträge in IT-Business:

Plattformen im Internet	Heft 4/2022
Self-Sovereign-Identity: Eine Chance für die Schweizer E-ID?	Heft 3/2022

Diverse Beiträge in IT Spektrum:

EU – U.S. Data Privacy Framework	Heft 1/2023
Metaverse – parallele Welt(en)	Heft 6/2022
Regulierung Künstlicher Intelligenz (KI)	Heft 5/2022
Digital Services Act (DSA)	Heft 4/2022
GPS-Tracking von Geschäftsfahrzeugen	Heft 3/2022