@ TEMET - About & Beyond Trust

World Wide Trust

- André Clerc
- Dipl. Inf.-Ing. FH, CISSP, CAS PM
- TEMET AG, Zürich

Bern, 29. März 2022

Agenda

- Digital IDs in a World Wide Context
- Digital Representation of Human Being
- Challenges in Digital ID Systems/Programmes
- Principles on Sustainable Identification
- Safeguards
  - Self Sovereign Identity Model
- Unresolved Challenges

Digital ID Use Cases

- Digital ID as credential → government
  - Corresponds with specific information that someone can identify themselves with
    → Birth certificate, social insurance/security number, passport, driver's license, …

- Digital ID as user (name)
  - Corresponds to a collection of information associated with a person's digital behaviour
  - Created by a counterparty that an entity interact online with

- Digital ID as avatar (character)
  - Self-created digital ID, which has more or less to do with the data of the creator

- Digital ID as reputation (title)
  - Compiled by authorized or reputable entities
  - Contains information about an individual's history or track record in a particular area

Staatliche E-ID

(Source ⧉)

Digital IDs in a World Wide Context

Staatliche E-ID

(Source ⬀)

European Digital Identity (EUDI) Wallet

(Source ⧉)

World Population (2018)

Internet using
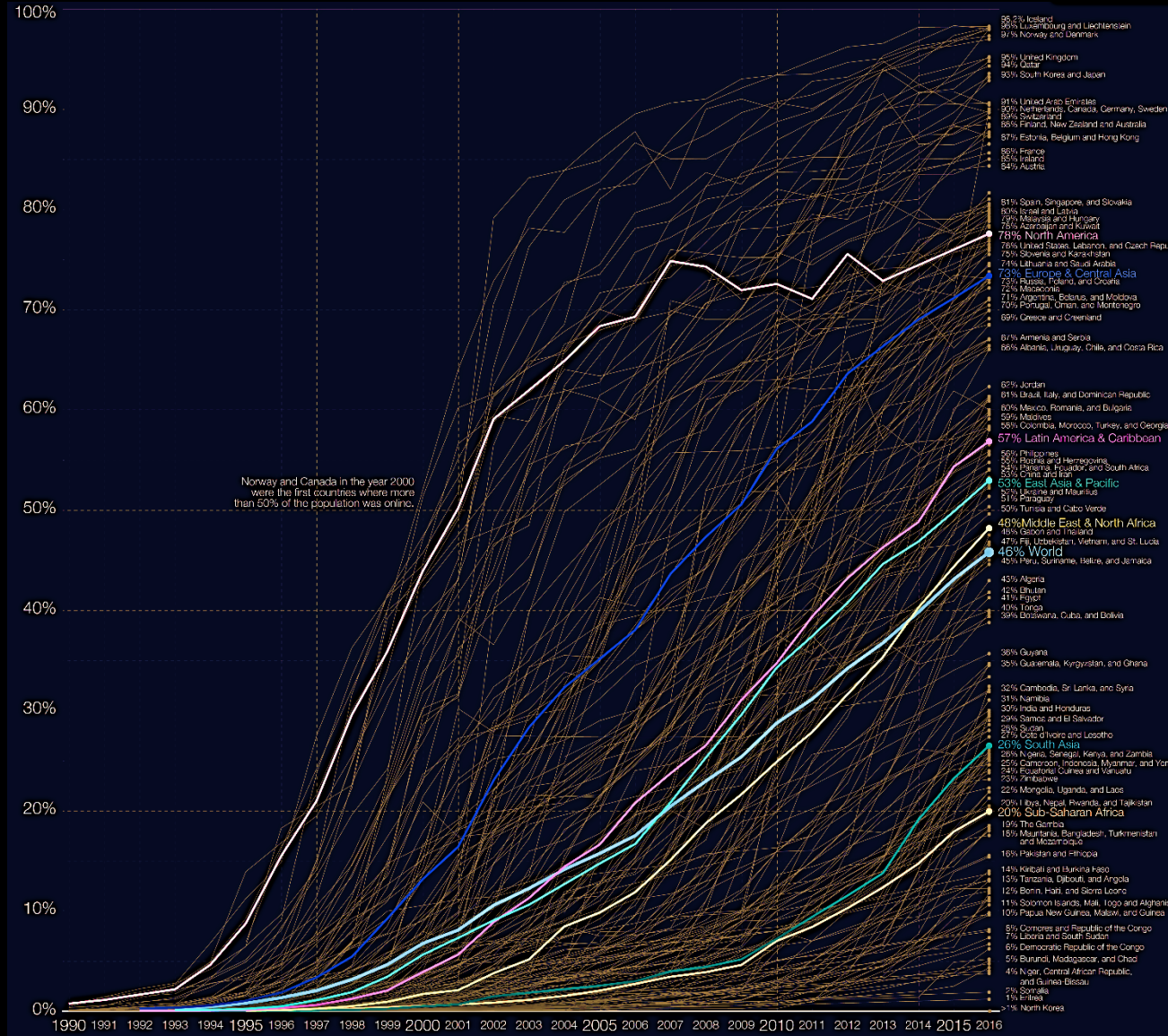
>97% Iceland, Luxembourg, Liechtenstein, Norway & Denmark

78% North America
73% Europe & Central Asia

57% Latin America & Caribbenan
53% China

46% World Wide

30% India

2024 5-Billion
LMIC, Asia & Africa

(Source ⬀)

Digital ID Systems

- Governments that have adopted centralised ID envision a single source of personal identity about every person in their jurisdiction
  - Countries adopting this model (Venezuela), are inspired by China
    → building a social credit system from digital ID.

- The largest national digital ID system is Aadhar (India)
  - Records **biometric & biographical** data of an individual and issues **a card with biometric** identity
    - identify them as they access government services
    - currently used for social welfare programmes (food distribution)
    - Private actors (banks) were also requiring it mandatory until this was limited (08.2017)

- High income countries (US, UK, …) have adopted decentralized digital ID systems
  → Estonia sophisticated, federated digital ID system

Digital Representation of Human Being
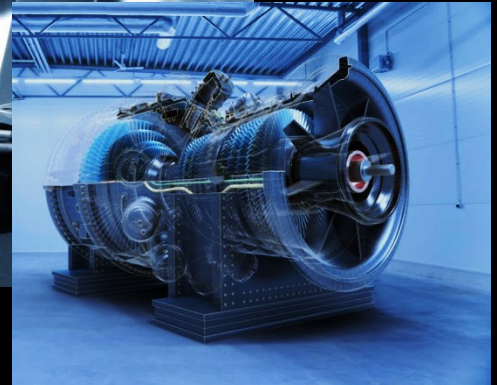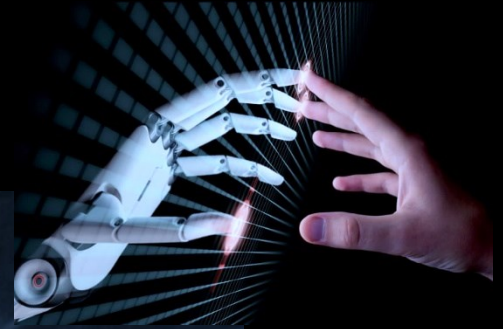
Digital ID Definition

- The term digital identity (DI, digital ID) can sometimes be quite confusing because its definition depends on the underlining and is not yet standardized
  - National Institutes of Standards and Technology (NIST)
  - World Economic Forum (WEF)
  - World Bank

- Digital IDs: The way a human is represented online & digitally documented

- Digitally authenticated and stored collection of characteristics associated with a uniquely identifiable human

Digital Representation of Human Being

Digital ID Definition

- Universally accepted characteristics (not conclusive):
  - Must be personal and non-transferable (only the "owner" has the right to access & use it)
  - Is reusable
  - Is convenient (access & use it whenever you want without technical expertise)
  - Fulfills its intended purposes by allowing the execution of specific actions

- Multiple distinct identifiers can make up a digital IDs
  - Passport or Driver's license
  - Social (Security) numbers
  - Email addresses
  - Nicknames or abbreviations of first and last names
  - ...

- Digital ID are context-specific and may vary from organisations

Digital Representation of Human Being

Identification and Authentication

- Digital ID involves both identification and authentication of entities (humans & things)

- To identify a entities, they are **required to be enrolled**
  - Bind a collection of information to an digital ID
  - Their identifiers must be **stored in a database** for future reference

- Main approaches to authentication entities:
  - something that entities **knows**   → a secret number
  - something that entities **has**   → a mobile phone
  - something that entities **is**   → their physical features (**biometric, strong ID-Binding**)
                                           Kenya, South Africa & UK, have attempted to collect DNA

Digital Representation of Human Being

Identification and Authentication

- Technologies applied in digital ID:
  - Biometric   → fingerprints, earlobes, iris, face an most recently DNA
  - GPS   → track entities' locations
  - Artificial Intelligence → facial recognition software is used to process data collected

- Data collection & store
  - The collecting & storing data is and will be an enormous challenge (→ biometric)
    - China, Estonia, Ghana, & Philippines issue cards that stores personal information
    - Nigeria are using mobile phones and apps

- Why Biometirc?
  - Strong evidence that someone is who they claim to be → expensive

Challenges for Digital ID Programmes

Challenges for Digital ID Programmes

Privacy, Protection & Security

- Digital ID
  - Increases government surveillance capabilities
  - Providing the means to monitor and stifle dissenters
  - Politically manipulate sectors of the population
  - Provide services discriminately

- Intersection of legal identity with technology has raised many concerns
  → Privacy & Data Protection

- Design of the digital ID programmes (DBs, Access & Permissions)
  → easily override the right to
     informational self-determination and autonomy
  - Especially by centralise data collection

Trust in Digital ID

- A basically good idea Single Source of Truth (single provider model) gets askew
  - It is at odds with responsible data sharing practices, particularly when a data protection framework is missing

- Digital ID have enormous influence potential or could serve as a means of information control
  - Digital ID Databases in the wrong hands or control can easily become a danger or be weapinise against a country

- To ensure that digital ID information are used for its intended purpose, it is mandatory to implement appropriate safeguards

Challenges for Digital ID Programmes

Freedom, Equality & Fraternity

- More as 1 billion people do not have basic proof of identity
  → Essential for protecting rights & enabling services access

- Many more:
  – Have forms of identification that are insecure or untrusted by service providers
  – Live in countries where identification systems are unsuited for the digital era or fail to safeguard people's rights and data

- Improving accessibility, quality & governance of ID systems is critical for inclusive development

Sustainable Identification

Frameworks

Guidelines

Principles

Sustainable Identification

Principles

- The World Bank published with over 30 organisations the principles on sustainable identification (Source)

African Development Bank	OSCE Office for Democratic Institutions and Human Rights (ODIHR)
Asian Development Bank (ADB)	Plan International
Bill & Melinda Gates Foundation (BMGF)	Privacy and Consumer Advisory Group to the Government Digital Service and GOV.UK
Center for Global Development (CGD)	
Digital Impact Alliance (DIAL)	Secure Identity Alliance (SIA)
Digital Nations	Smart Africa
FHI 360	The GSMA
ID2020 Alliance	Tony Blair Institute
ID4Africa	UN World Food Programme
International Organization for Migration (IOM)	UNHCR, The UN Refugee Agency
International Telecommunication Union (ITU) International	United Nations Capital Development Fund (UNCDF)
Union of Notaries	United Nations Children's Fund (UNICEF)
Mastercard	United Nations Development Programme (UNDP)
Norwegian Agency for Development Cooperation (Norad)	United Nations Economic Commission for Africa (ECA)
Omidyar Network	Women in Identity
Open Identity Exchange UK/Europe	World Bank Group
Organization of American States	

- Ambition for every person/human:
  - Right to participate fully in their society / economy
  - Be recognised as a person before the law

Sustainable Identification

Principles on Identification for Sustainable Development (Source ⬈)

Inclusion
| 1. | Ensure universal access for individuals, free from discrimination |
| 2. | Remove barriers to access and use |

Design
3.	Establish a **trusted–unique**, **secure**, and **accurate–identity**
4.	Create a responsive and interoperable platform
5.	Use **open standards** and prevent vendor and technology lock-in
6.	Protect **privacy and agency** through system design
7.	Plan for financial and operational sustainability

Governance
8.	Protect **personal data**, maintain **cyber security**, and **safeguard people's rights** through a comprehensive legal and regulatory framework
9.	Establish clear institutional mandates and accountability
10.	Enforce legal and **trust frameworks** through independent oversight and adjudication of grievances

Digital ID

Safeguards

Digital ID

Safeguards

- Digital ID systems should
  – Follows the necessary cyber security standards NIST CSFW, ISO/IEC 27K
  – Privacy & security by design (on-prem/cloud)
  – user-centric → give people control over who accesses their data
  – able to preserve information (effective & efficient)

- Among solutions being proposed:
  – Shifting the control from government and private actors to the person
  – Requires that digital ID systems are designed for privacy
    → giving the person control over who accesses their data

- Self Sovereign Identity (SSI, @TEMTE 2022⤢), where individuals store their digital ID in "wallets" & provide their identity data when needed

Digital ID

- Self Sovereign Identity (SSI, @TEMTE 2022), where individuals store their digital ID in "wallets" & provide their identity data when needed

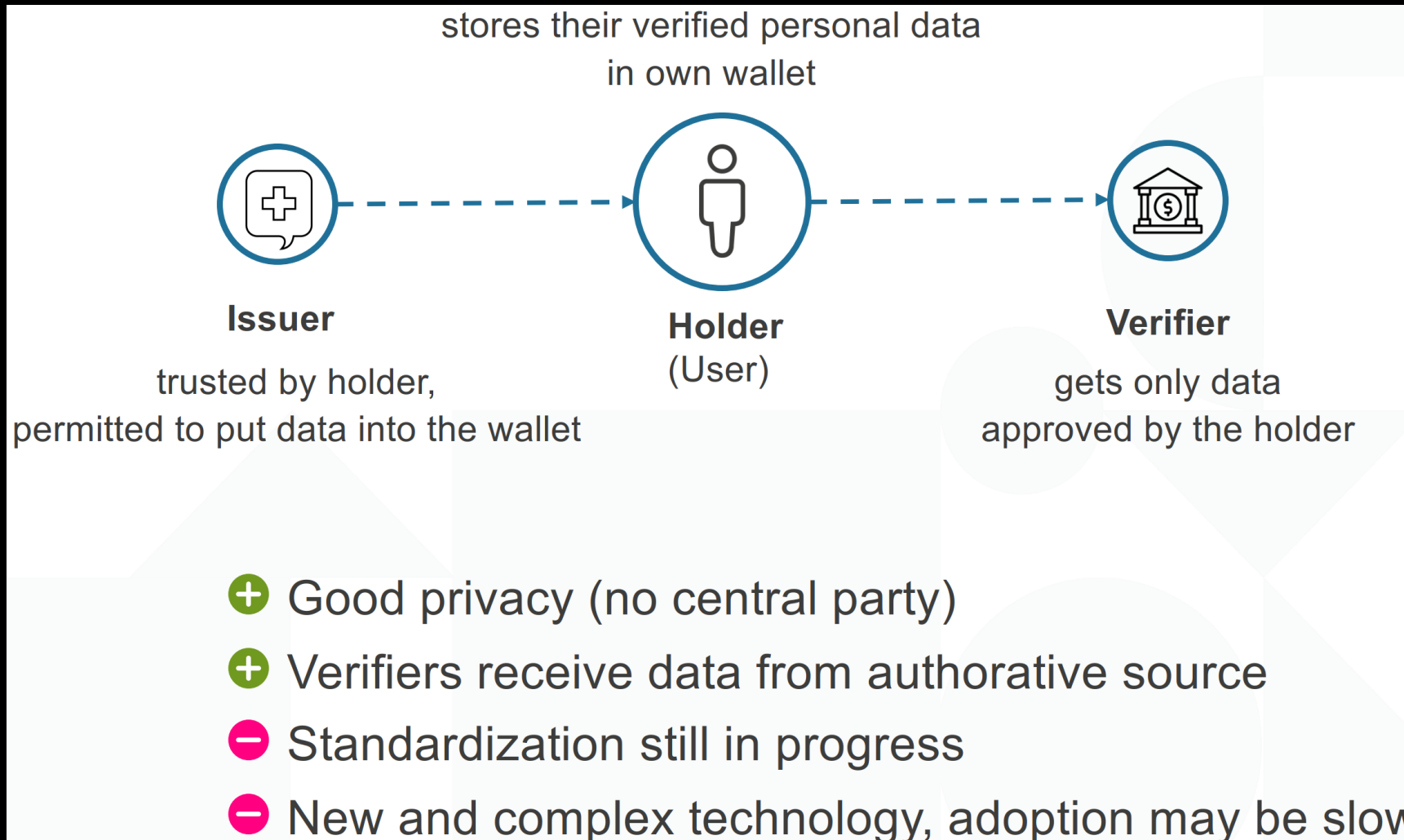- Once produced, a digital ID is used for authentication but not stored with the service provider

- Built around principles of control:
  - Access
  - Consent
  - Interoperability
  - Minimisation
  - Persistence
  - Portability
  - Transparency
  - User protection
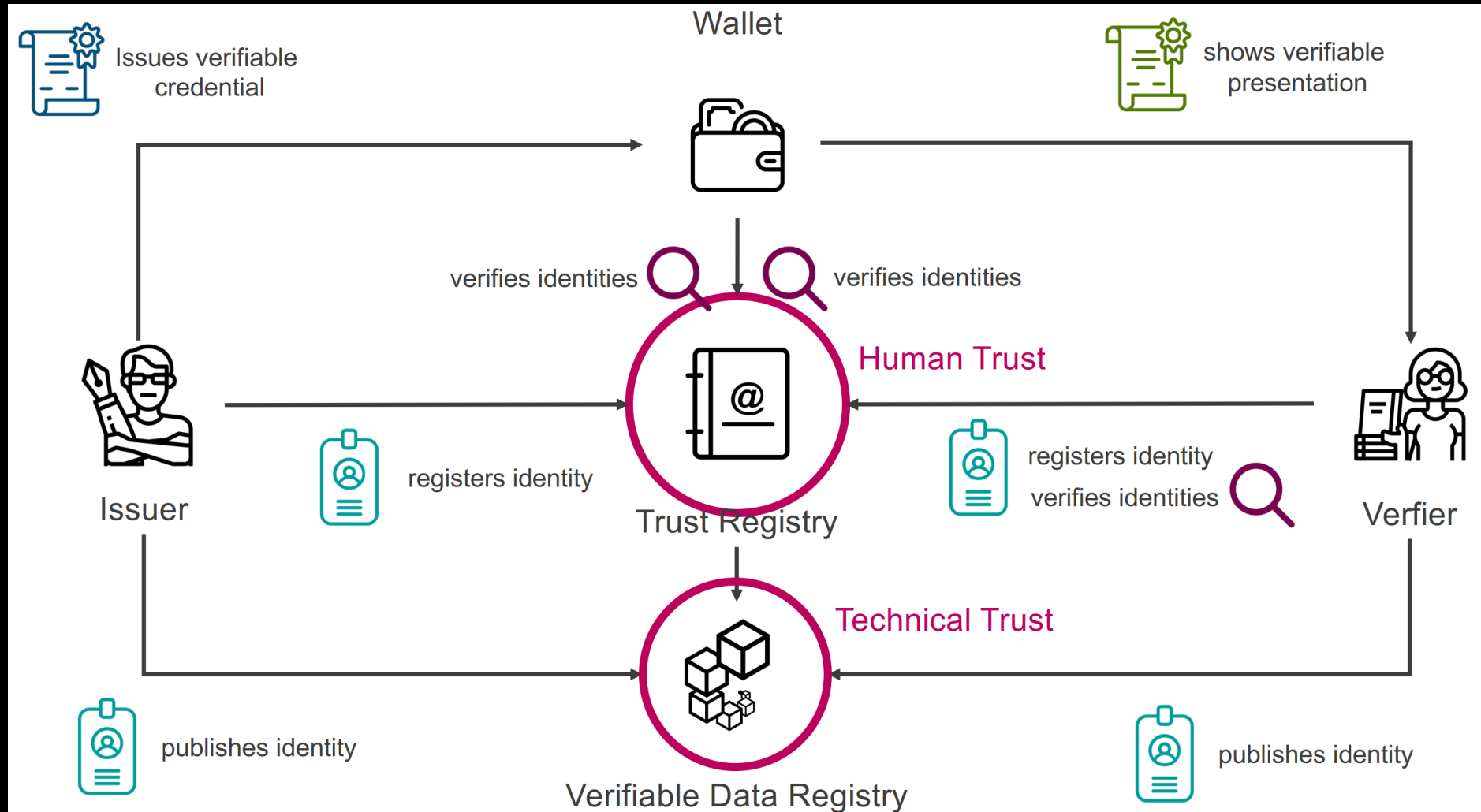
Safeguards - Self Sovereign Identity

(Source ⬀)

stores their verified personal data
in own wallet

Issuer

trusted by holder,
permitted to put data into the wallet

Holder
(User)

Verifier

gets only data
approved by the holder

- ➕ Good privacy (no central party)
- ➕ Verifiers receive data from authorative source
- ➖ Standardization still in progress
- ➖ New and complex technology, adoption may be slow

Safeguards - Self Sovereign Identity Model

Trust in the Communication counterpart

THANK YOU
FOR
YOUR
ATTENTION