



DIDAS

Daniel Saeuberli

daniel.saeuberli@didas.swiss

December 2023

Who are we and
why should you care?

Approx
3 Years Ago,
September
9th 2020



We founded the DIDAS Association to give Swiss citizens and our children a choice. To empower them with the tools to one day be able to maintain sovereign control over their data in a time of digital ubiquity.

By following something called SSI Principles to, step-by-step on a long winding road, help establish Authenticity, Verifiability and Trust (which the world needs to function), but without compromising privacy (which we urgently need to continue functioning).

We were fortunate to be right.

We are an inclusive group of professionals, experts and enthusiasts - you and your organisation can join us too.

We help to create value for a wide range of stakeholders.

The initiative holds true societal AND business value.

The Privacy Paradox

The "privacy paradox" refers to the situation where individuals express concerns about their privacy but do not take significant actions to protect it, often sharing personal information freely online.

Yes, I value my privacy highly!

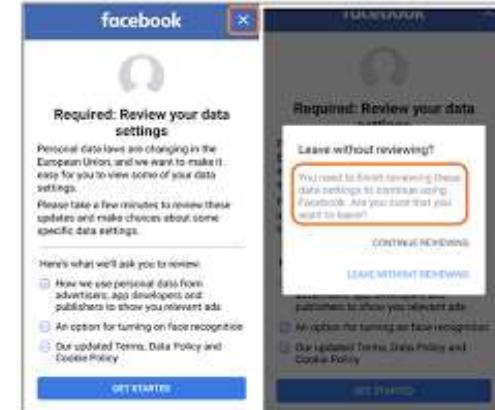


No so fast!

Distorting Influences

- biases and heuristics
- framing effects
- behavioural manipulation and skewing

Go ahead Facebook,
I agree to all your terms 😊

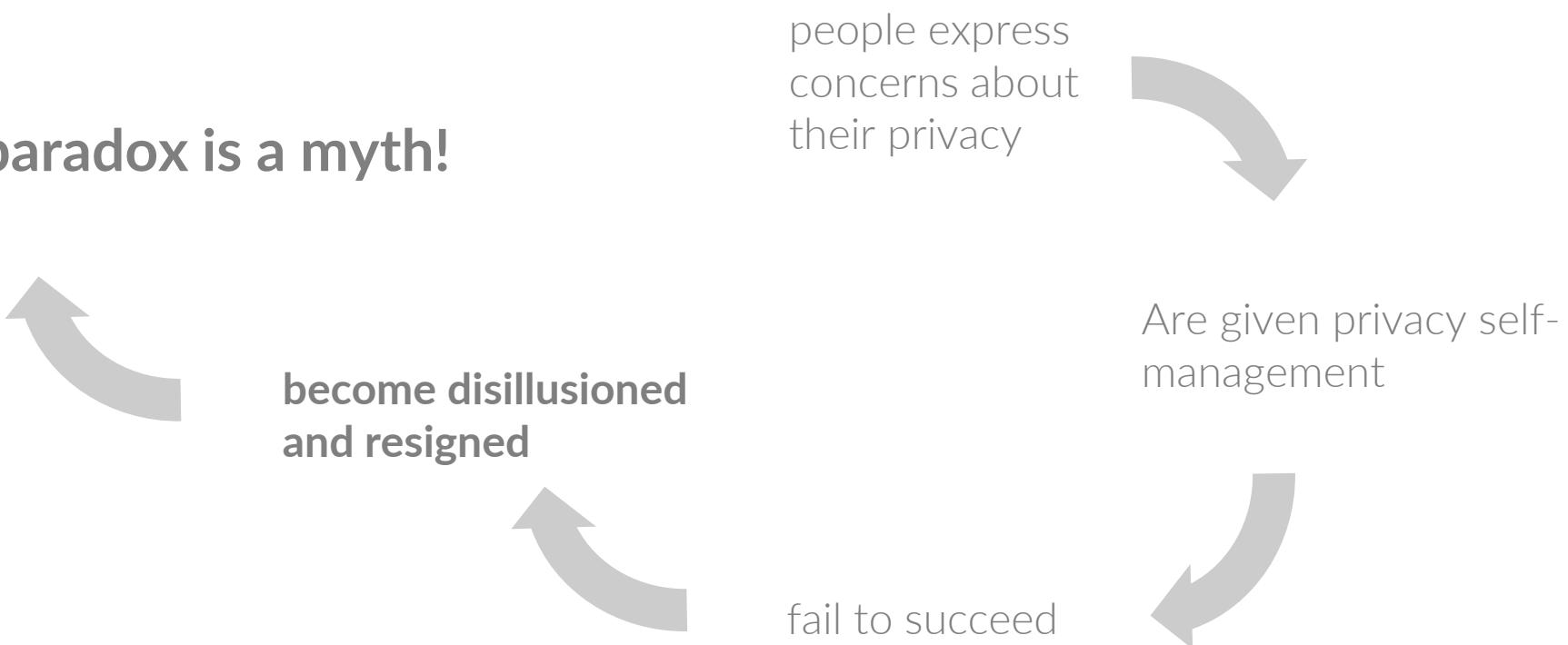


The Takeaway

This phenomenon is complex, influenced by various factors like convenience, lack of awareness, or the perceived benefits of sharing data.

It is not just about contradictory behaviour but more so about the environment in which individuals make their privacy decisions.

Actually: The privacy paradox is a myth!



We need better



tools (e.g. Advanced Cryptography
and Privacy Mechanisms)

design principles

enabling technologies

legal frameworks

DIDAS Good SSI Practices¹⁾

Right for digital Identity and Agency,
freedom of choice and portability.

Ability to Delegate / Guardianship

High data protection with minimal disclosure



Coercion-free and self-sovereign

User-friendly with added value

Safely decentralized

Transparent interoperability

Trust in data and information, globally

1) In Anlehnung an WEF – Identity in a Digital World A new chapter in the social contract ([WEF_INSIGHT_REPORT_Digital Identity.pdf](#) (weforum.org)), Christopher Allen – The Path of Self-Sovereign Identity ([The Path to Self-Sovereign Identity](#) (lifewithalacrity.com)) und Sovrin – Principles of SSI ([Principles of SSI – Sovrin](#))

We value deep representation of key aspects in the eID Initiative

The draft law and today's published "discussion paper on Initial technological basis" for the Swiss trust infrastructure, represent a comprehensive and wise approach to developing a Swiss e-ID system that respects privacy, ensures data minimisation, involves public discussion and remains open to technological evolution. Let's keep it up!

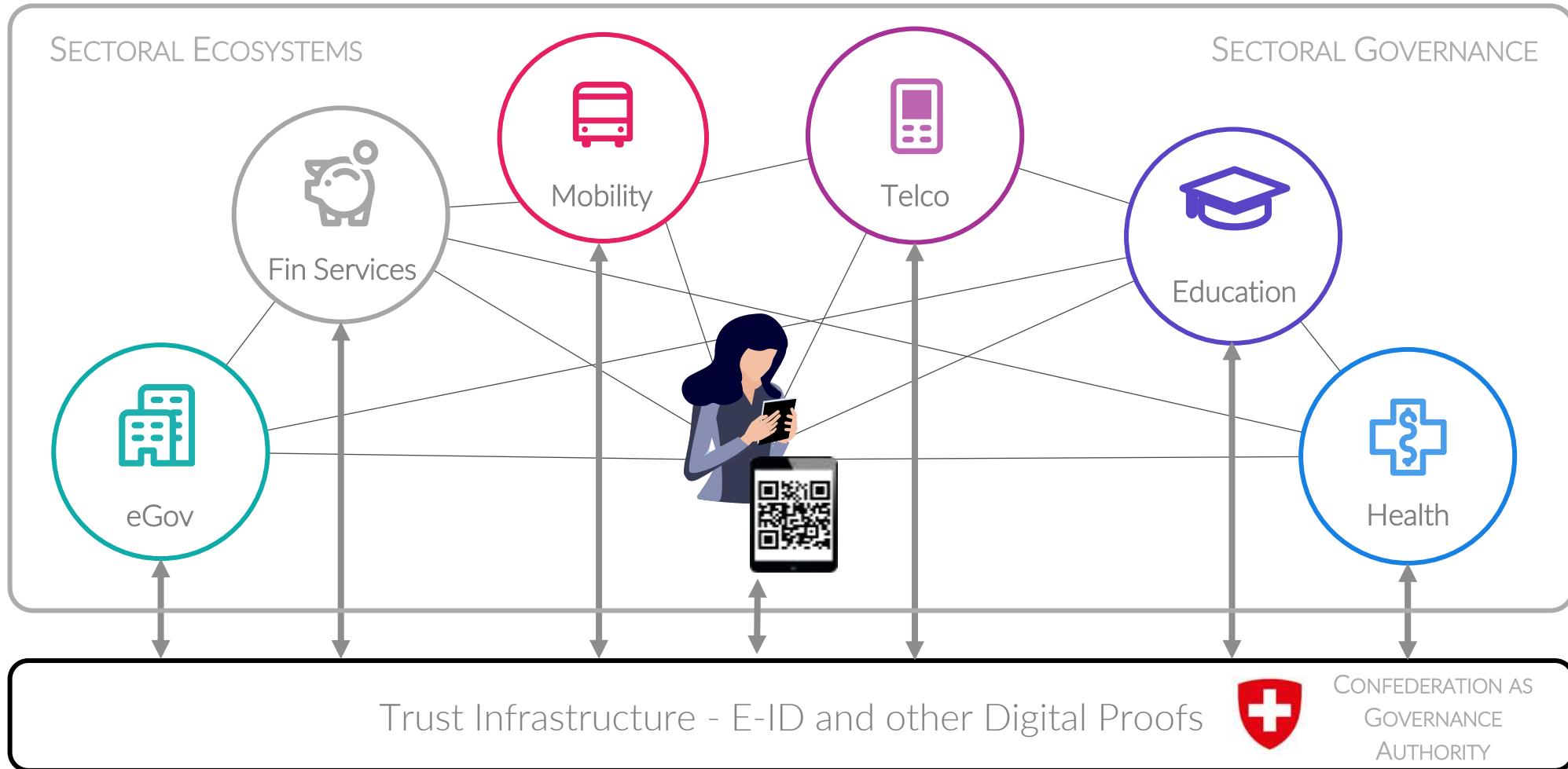
- Privacy by Design, Data Minimisation, Decentralised Data Storage
- Self-Sovereign Identity Principles
- Public Discussion and Involvement
- Interoperability and International Compatibility (Step-by-step)
- Technological Neutrality
- Use of Modern Cryptography and Protocols

The Value of Verifiable Credentials is hidden and substantial

We help it come to life in use-cases

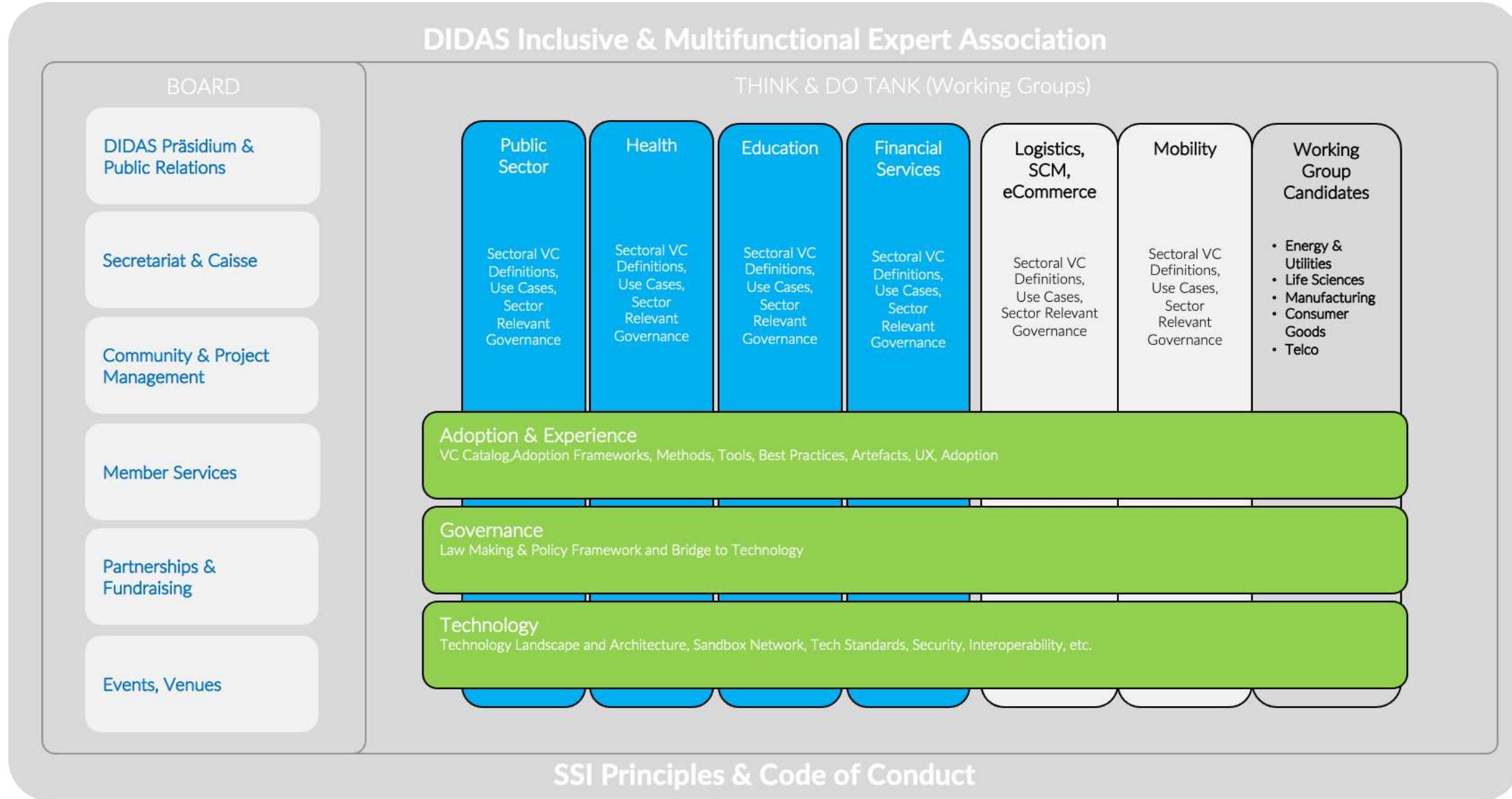
- New Businesses & Models
- Enhanced Efficiency and Speed
- Improved Security and Fraud Prevention
- Increased Trust and Transparency
- Verifiability across Networked and Chained Data Flows
- Cost Reduction, e.g. through removing friction, etc.
- User-centric service design removes complexity

Trust Infrastructure and Sectoral Ecosystems go Hand-in-Hand



Sectoral governance/regulations only need to be adapted to enable the possibilities of digital proofs

Association Structure: Board, Working Groups & Facilitators

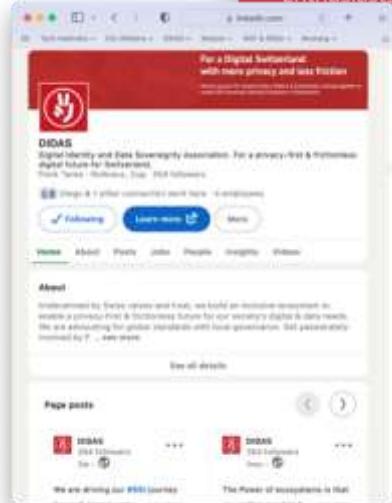


How we work:

- Open & inclusive
- All-Hands Community Calls
Fortnightly on Friday
- Alternating Fortnightly
Working Group Calls & Meets
- 1-2 quarterly, physical meetup
of DIDAS members and friends
- Community Platform
- DICE – Digital Identity
Unconference
- Visit of 3-4 conferences or
national / international events
with participation of
DIDAS members.

www.didas.swiss

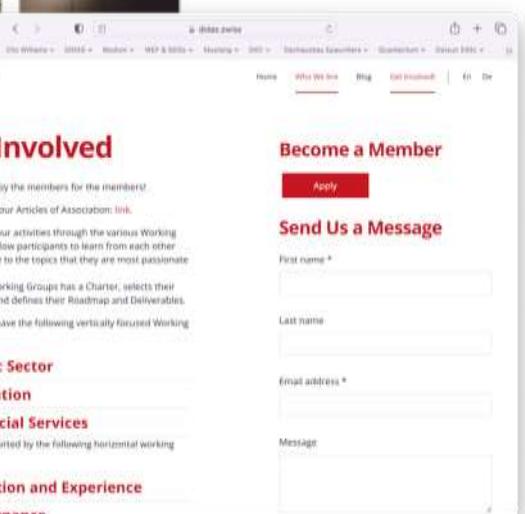
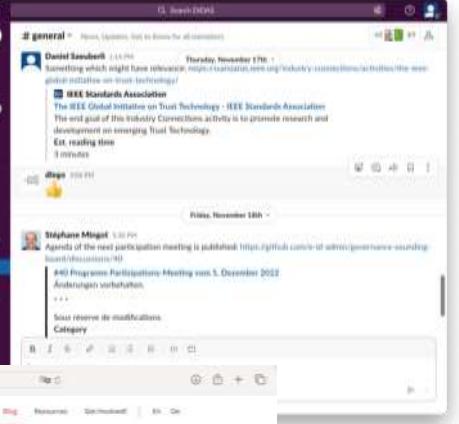
LinkedIn



GitHub



Slack



How we work: Impressions from DICE



Our Contributions So Far: 2023 and Before

- Development of SSI principles, demonstrations, and proof of concepts based on real-world use cases
- Digital Identity Unconference (DICE Europe) 2023 with over 160 participants. Join us in 2024!
- Collaborations in cross-sector environments including national and international public, private and academic stakeholders
- Collaboration with digitalswitzerland on a joint view of how an SSI ecosystem could look like
- Contributions to the Swiss E-ID law draft and with practical tools for the Swiss SSI ecosystem
- Standardization of key verifiable credentials
- Setting up a VC catalogue and an education concept (101 of E-ID)
- Contributions to the EPD Lawmaking Process
- Broadly disseminated viewpoint on the ARF
- Contributions to International Collaboration and Transparency
- Founding member of the OpenWallet Foundation
- Disseminating best practices and solutions in secure supply chains and digital trust with ICC and GLEIF support.
- DIDAS Members actively helping to re-wiring the Swiss Healthcare landscape
- Members active in establishment of Pan-European Educational VC Ecosystem

Outlook

- Continue to be a Principles and Values-driven, independent help to Switzerland
- Addressing challenges in digital trust, tech stack, governance, and Political, public, business literacy
- Institutionalizing our work with your help

A huge thanks to all of you!

Join us so we can build lots of
T(h)rust!

WEF 2024 Identity Day
17. January 2024, Davos



DICE 2024
18.-20. Juni 2024, Zurich



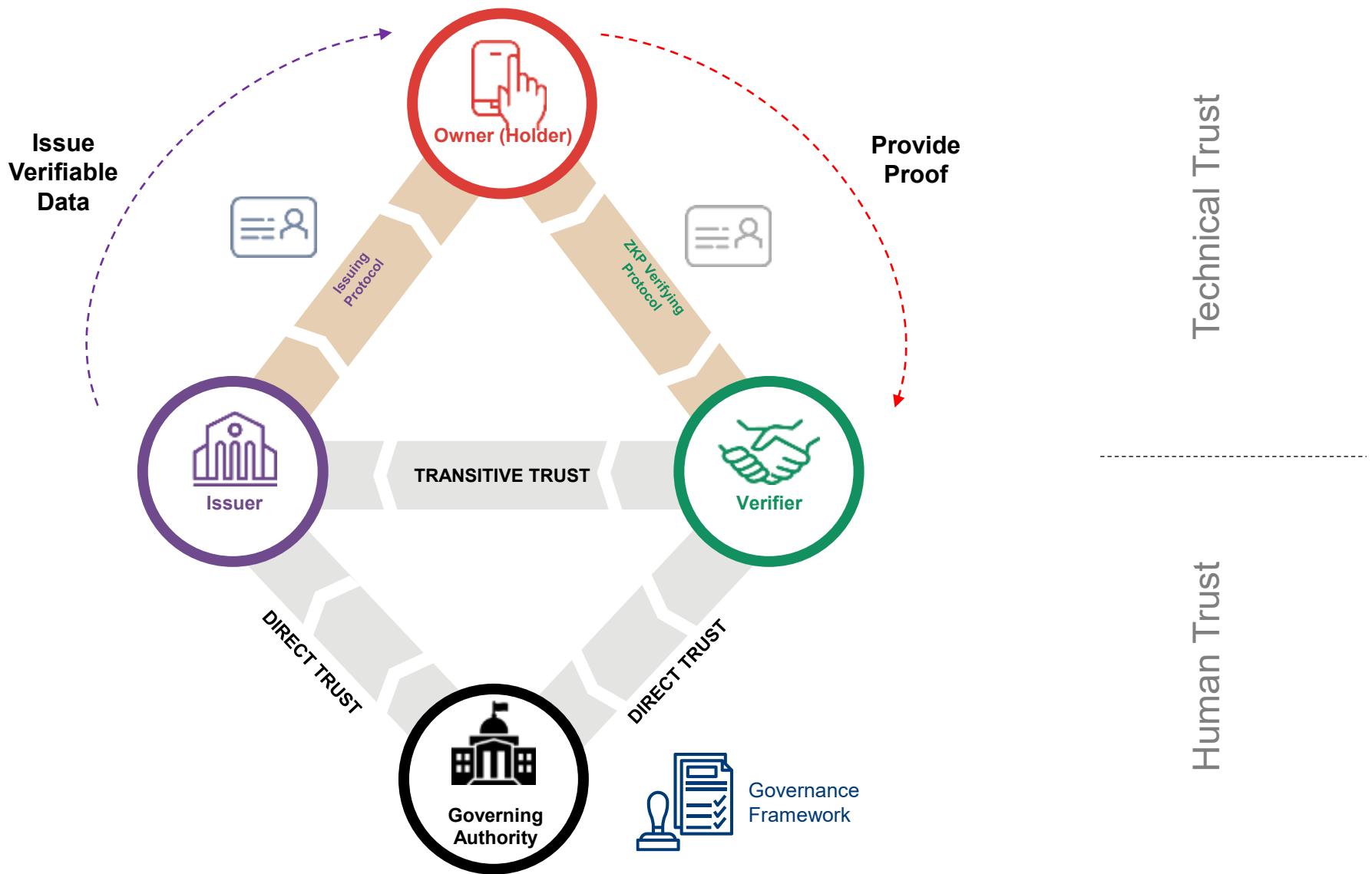
DIDAS

www.didas.swiss

December 2023

The road ahead of us

TRUST DIAMOND



Summary of SSI Practices – 1/2

Right for digital Identity and -Agency, freedom of choice and portability.

The SSI ecosystem ensures that every entity (people, companies, objects, etc.) can be represented in the virtual space by one or more digital identities (inclusion). The entity should be granted the right to freedom of choice and decisions should not have a discriminatory effect. This freedom of choice also includes the right to a barrier-free change of provider.

Coercion-free and self-sovereign

The SSI ecosystem ensures that entities can freely reveal their identity or parts of it. Furthermore, it enables the use and release of digital identity data to be carried out by the owner in a controlled manner. The identity owner has full transparency of what he/she has shared with whom and can delete or update his identity data and relationships at any time.

Ability to Delegate / Guardianship

The SSI ecosystem ensures that entities are enabled to delegate the representation and use of their identity to third parties (other people, organizations, devices, etc.). In particular, it ensures that people who are disabled or not of age do not experience any disadvantage.

User-friendly with added value

The SSI ecosystem ensures that the application of the digital identity is simple, intuitive and consistent. It should not only focus on partial aspects (e.g. authentication) but should provide the owners with comprehensive added value. An ability to use in multiple situations (frequency) contributes to an increased attractiveness - and vice versa.

1) Adapted from WEF – Identity in a Digital World A new chapter in the social contract ([WEF_INSIGHT_REPORT_Digital Identity.pdf \(weforum.org\)](#)), Christopher Allen – The Path of Self-Sovereign Identity ([The Path to Self-Sovereign Identity \(lifewithalacrity.com\)](#)) and Sovrin – Principles of SSI ([Principles of SSI – Sovrin](#))

Summary of SSI Practices – 2/2

Safely decentralized

The SSI ecosystem ensures that the participants are not dependent on a central system. There is no central authority that generates digital data without the consent of the identity holder (“shadow information”), organizes, controls or verifies the exchange. The SSI ecosystem enables owners to save data and transactions, manage cryptographic features (identifiers, keys) themselves and establish encrypted communications with the other owners.

High data protection with minimal disclosure

An SSI ecosystem ensures that the entity's privacy and integrity are always protected, that unauthorized third parties have neither access nor insight into the identity data and its use (privacy by design) and that the identity holders have to disclose only the part of the data that is required for the Business application/transaction in question.

Transparent interoperability

The SSI ecosystem ensures that the request and storage, presentation and exchange as well as the verification of identity data within the ecosystem and in interaction with other ecosystems are designed to be interoperable and transparent. All participants should have the right to gain insight into the necessary information so that they understand the conditions under which the ecosystem works. This is made possible by the application of uniform, open and international standards.

Trust in data and information, globally

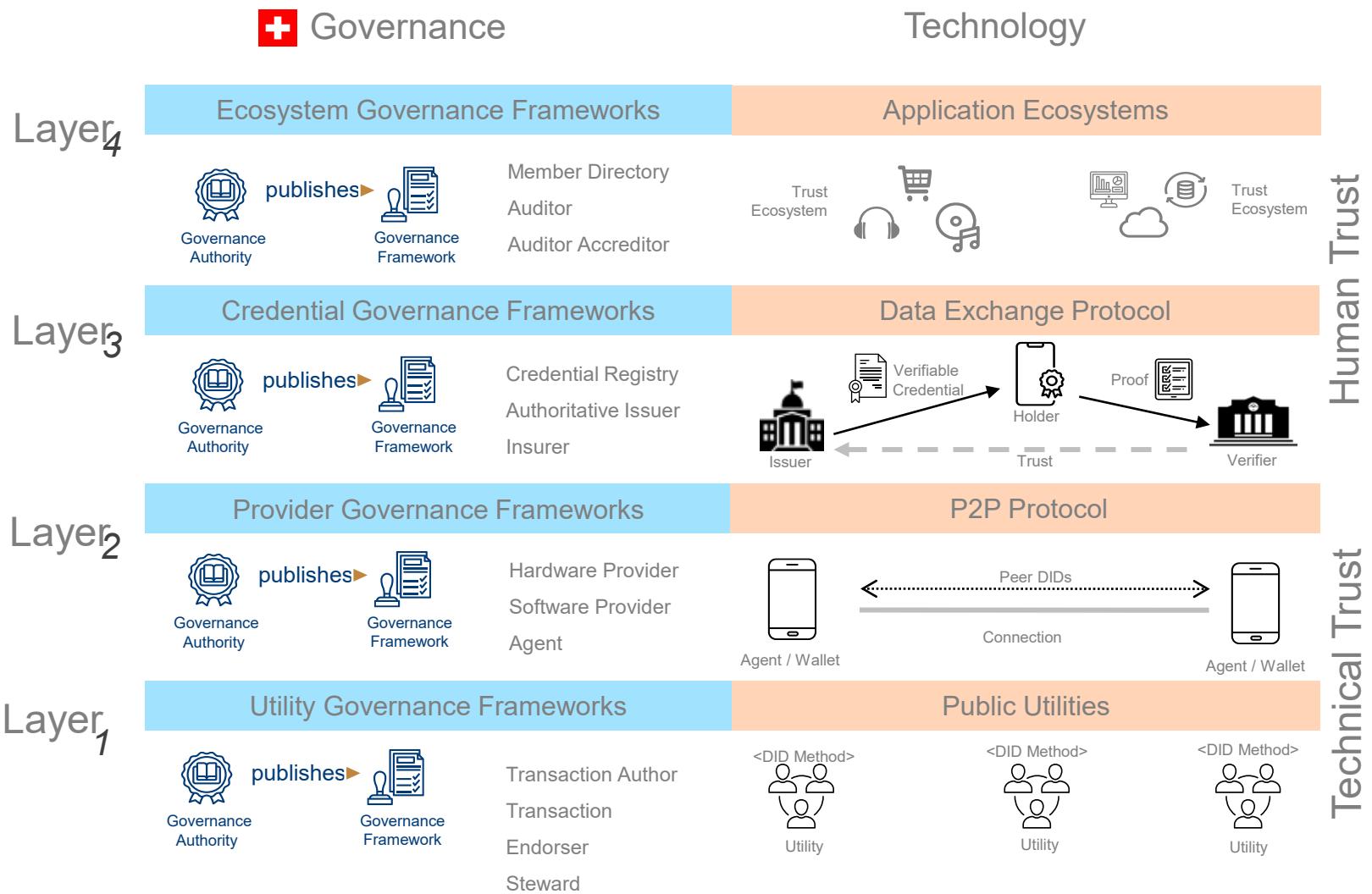
An trust ecosystem must ensure that there is trust between the participants. Identity holders should be able to present identity data in a tamper-proof manner whether they are Individuals, Organisations or Machines. Recipients of identity data should be able to check the authenticity of the data they receive to ensure that they come from an authentic source.

1) Adapted from WEF – Identity in a Digital World A new chapter in the social contract ([WEF_INSIGHT_REPORT_Digital Identity.pdf \(weforum.org\)](#), Christopher Allen – The Path of Self-Sovereign Identity ([The Path to Self-Sovereign Identity \(lifewithalacrity.com\)](#)) and Sovrin – Principles of SSI ([Principles of SSI – Sovrin](#))

Recommendation for Institutionalized Competency

Focusing on adoption, value creation for private sector, and Switzerland's contribution to a more trusted global digital realm:

- Establish independent expert bodies for governance & technology and usability recommendations with diverse, multifunctional backgrounds.
- Actively Enhancing Adoption Early through Private- & Public Sector Value Creation Support (digital transformation enablement)
- Pro-active educational initiatives at scale for enhanced understanding of the new paradigms across stakeholders
- Systematically support acceleration of technological innovations and agility through experimentation
- Actively contributing to international standards and tools (e.g. advanced cryptography and privacy mechanisms)



RECAP - CREATING FOUNDATION FOR TRUST

Global Standards & Local Governance