Participation Meeting E-ID
May 5th, 2022

digitalswitzerland

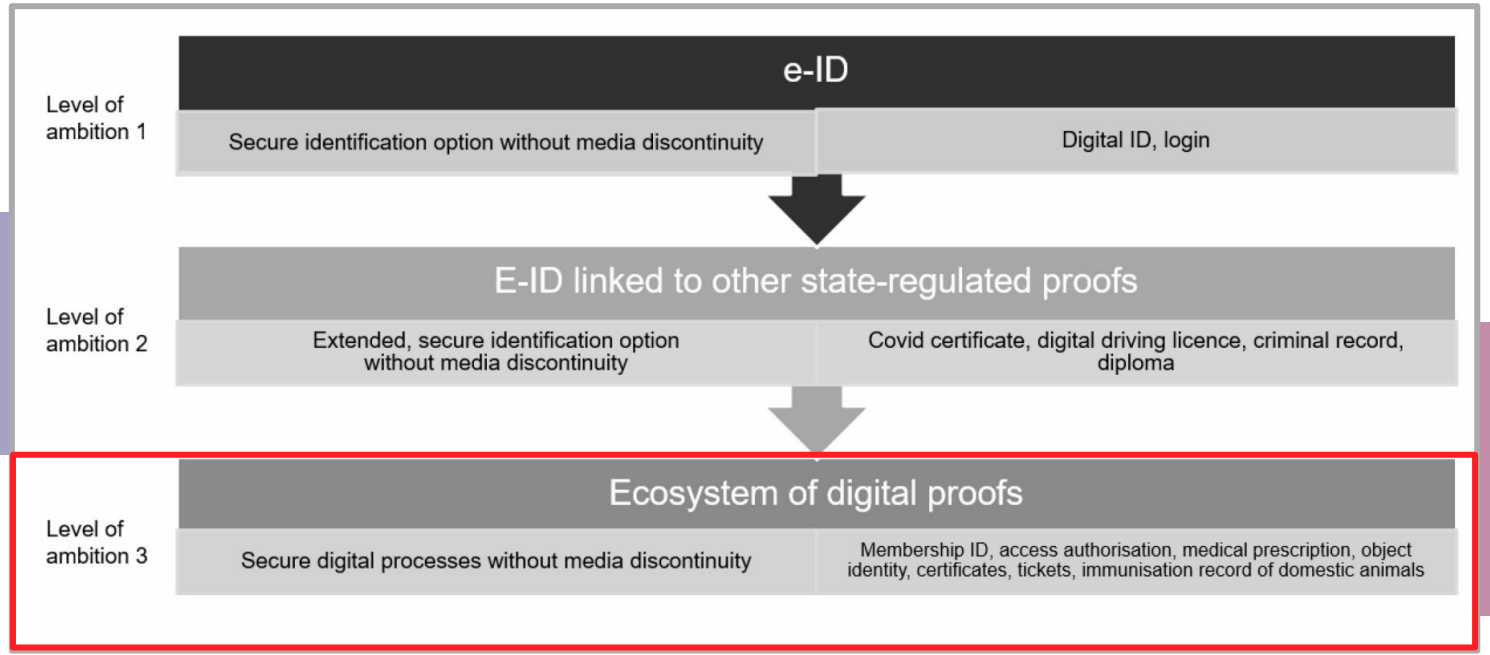
MAKING SWITZERLAND
A LEADING DIGITAL
INNOVATION HUB

Agenda

Item	*Time*
How is dCH contributing?	5min
What are our main points?	5min
Short Q&A	5mi

How are we contributing?

Restart via Public Consultation



E-ID Topic Directional Decision Federal Council

- **Grundsätze für die Ausgestaltung eines künftigen staatlichen Identitätsnachweises (E-ID) festgelegt**
  1. Nutzerinnen und Nutzer sollen grösstmögliche Kontrolle über ihre Daten haben (**Self-Sovereign Identity**)
  2. Datenschutz soll gewährleistet werden durch
     - das System selber (Privacy by Design)
     - durch die Minimierung der nötigen Datenflüsse (Prinzip der Datensparsamkeit)
     - dezentrale Datenspeicherung
  3. E-ID soll auf einer **staatlich betriebenen Infrastruktur** beruhen
  4. Ausbau zu einem E-ID-Ökosystem erfolgt schrittweise
  5. Pilotprojekte zu einzelnen möglichen Anwendungen, z. B. Pilotprojektidee von ASTRA/asa: «digitaler Führerausweis»

Source: Press Release

What's the involvement of our members?

After a open call to our network for participation, 10 digitalswitzerland members have committed their digital identity expert for 4hrs/week for 3 Months

SBB CFF FFS

adnovum

HSLU Hochschule Luzern

swisscom

cisco

UBS

Allianz

Berner Fachhochschule

SWITCH

ti&m
big ideas. creative technology.

With support of

DIDAS

digitalswitzerland

What did we aim to do?

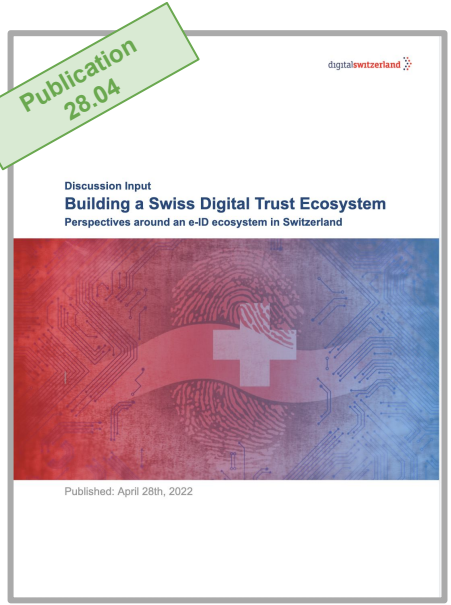
We launched an Expert Studio in early January to collaboratively produce a discussion input in the form of a white paper to complement the meta-level discussion.

Principles of the White Paper

1. It's a **discussion input** (not a formal academic study), which will **neither be perfect nor comprehensive** at time of publishing.
2. It's an **initial expert perspective** on the topic, across private sector and academia, to be **iterated upon in future versions.**
3. It's **bundling knowledge where there lies consensus**. For polarising topics, options are highlighted but no stance taken.
4. It's **understandable for the 'professional crowd'.** It is succinct, thus purposefully aimed to be rather short.

How are we contributing?

Over the past three months, these Experts have collaboratively wrote an initial discussion input

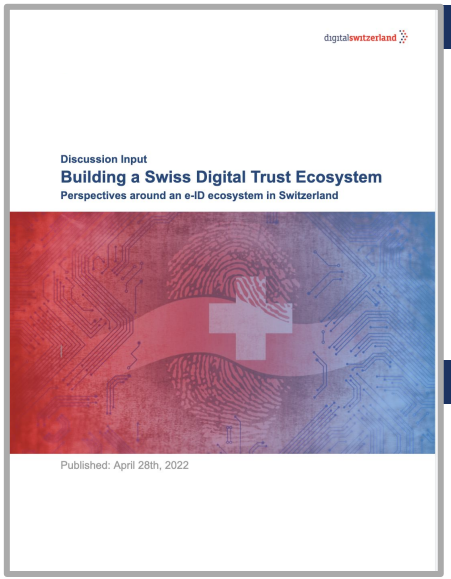


1. Where are we now in Switzerland? What are the relevant trends internationally?
2. Where could we be heading in Switzerland given the directional decision by the government?
3. What are relevant perspectives and lessons learned across the economic, technical, governance and legal dimensions?

What are our main points?

Teaser only ;-) read the whitepaper and let’s discuss via GitHub!

What are our main messages?



#1

Ein ‘Ecosystem of Digital Credentials’ (EDC) geht primär um Vertrauen
Um ‘Technical Trust’ zu schaffen, wäre ein **‘national, publicly licensed network’, ein sogenanntes Vertrauensnetzwerk,** mit einer von der Regierung benannten Aufsichtsbehörde zielführend.

Die Knotenpunkte (i.e. Nodes) sollten über mehrere Schweizer Organisationen verteilt sein, darunter die Regierung, Nichtregierungsorganisationen (NGOs), Universitäten und der Privatsektor.

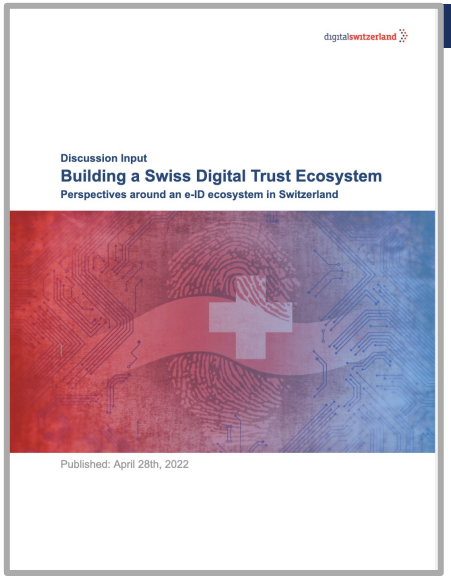
Read more in Chapter 2

#2

Nur direkt zu einem Ökosystem der Stufe 3 macht Sinn
Nur ein Ökosystem der Stufe 3, in dem es mehrere ‘Issuers’ und ‘Verifiers’ gibt (über den privaten und öffentlichen Sektor hinweg), **kann genügend Vorteile schaffen, um Investitionen und Risiken zu rechtfertigen**. Es würde Identitätsträger:innen in den Mittelpunkt stellen und dazu befähigen, über die eigene digitale Identität zu verfügen.

Read more in Chapter 3

What are our main messages?



3

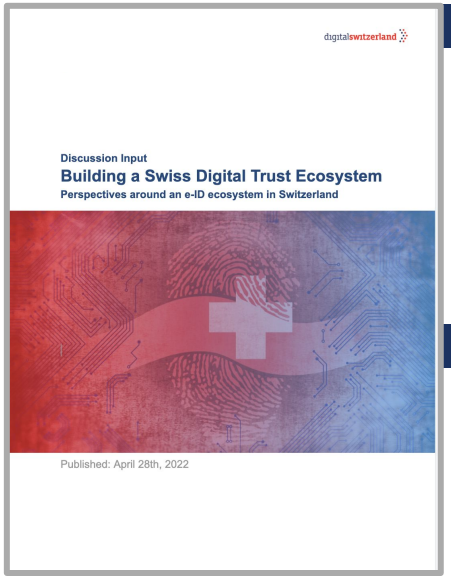
Technische Perspektive

Das e-ID-Ökosystem sollte nach den SSI-Prinzipien mit drei Rollen implementiert werden: User, Verifier und Issuer. Ein solches e-ID-Ökosystem soll durch **offene Standards**, **robuste Referenzimplementierungen** und einem von der Bundesregierung eingeführten Zertifizierungsprozess gewährleistet werden.

Auch die **Interoperabilität** muss auf den drei Anspruchsniveaus, zwischen den Ökosystemen des Sektors und in einer internationalen Perspektive durch die Verwendung gemeinsamer Standards durch alle Beteiligten gewährleistet werden.

Read more in Chapter 4

What are our main messages?



#4

Governance-Perspektive

Ein e-ID-Ökosystem sollte das **bestehende Vertrauen aus der analogen Welt in die digitale Welt übertragen**. Dies könnte erreicht werden, indem der Prozess der e-ID an denjenigen des Personalausweises angeglichen wird und bestehende Vertrauens-stellen eine entsprechende Rolle im EDC erhalten.

Read more in Chapter 5

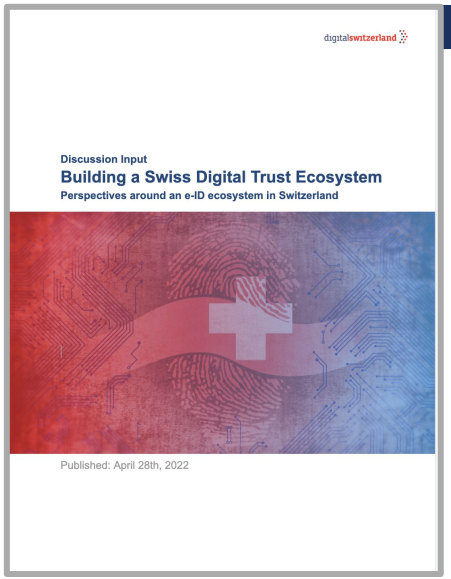
#5

Rechtliche Perspektive

Die Schaffung eines verlässlichen ‘Digital Trust Ecosystem’, in dem sichere Identitäten die Grundlage für den Rechtsnachweis bilden, ist für eine zukunftsfähige Digitalisierung notwendig. Es wäre sinnvoll, einen **Rechtsrahmen zu schaffen, der sich an internationalen e-ID-Lösungen, insbesondere denen der EU, orientiert.**

Read more in Chapter 6

What are our main messages?



#6

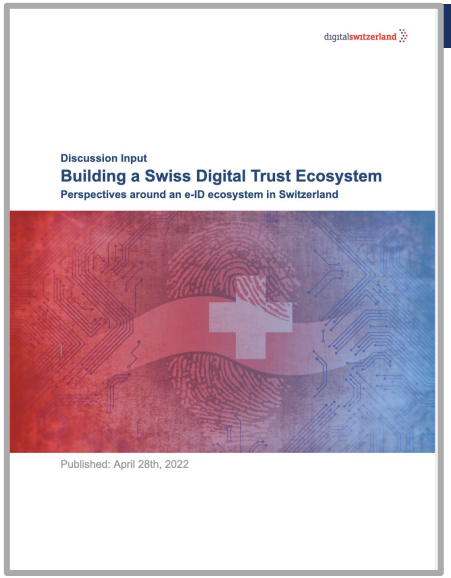
Benutzerfreundlichkeit

Ein e-ID-Ökosystem im Einklang mit den SSI-Prinzipien impliziert, dass **die Verantwortung für die Verwaltung der digitalen 'Wallets' und ihrer digitalen Nachweise, sogenannte Verifiable Credentials (VCs) auf den Nutzer übertragen wird.**

Die digitale 'Wallet' als zentrale Schnittstelle zur e-ID und den VCs ist besonders wichtig und sollte möglichst intuitiv sein. Die Ausstellung und der Entzug von VCs müssen also einfach, schnell und unkompliziert sein. Im Sinne der digitalen Inklusion müssen alle Bürger aktiv dabei unterstützt werden, die neuen Technologien zu verstehen und zu nutzen.

Read more in Chapter 7

What are our main messages?



#7

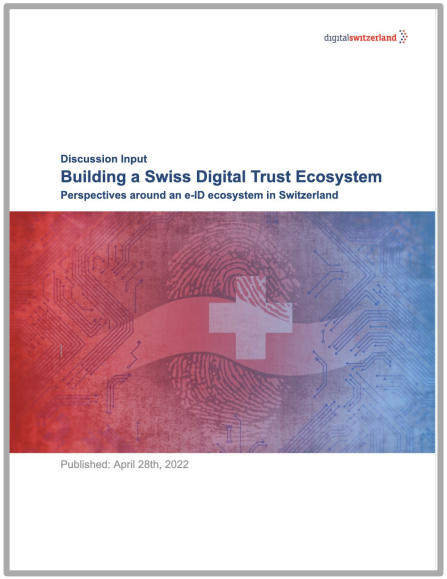
Benutzerfreundlichkeit

Beim Aufbau des e-ID-Ökosystems haben wir es mit einer **Version des *'chicken-and-egg problem'* zu tun, an dem drei Gruppen von Akteuren beteiligt sind,** anstelle der zwei Gruppen von Akteuren im klassischen *'chicken-and-egg problem'*.

Der entscheidende Faktor im *'chicken-and-egg problem'* ist die Anzahl der Use Cases. Solange diese Zahl niedrig ist, gibt es für die Akteure kaum einen Anreiz, sich am Ökosystem zu beteiligen. Es gibt mindestens sechs Grundsätze für Anwendungsfälle innerhalb eines e-ID-Ökosystems.

Read more in Chapter 8

Questions?



1. Where are we now in Switzerland?
   What are the relevant trends internationally?

2. Where could we be heading in Switzerland given the directional decision by the government?

3. What are relevant perspectives and lessons learned across the economic, technical, governance and legal dimensions?

Let's talk about it!

The primary goal is to initiate a discussion that is broad and inclusive.
The Whitepaper has been posted to the Github Forum. Let us know your thoughts!

digitalswitzerland

Appendix I

Figure 1

In the public consultation, the federal government outlined three distinct levels of ambition

Source: Swiss Federal Government

Ambition Level 1	**e-ID**	
	Secure identification option without media discontinuity	Digital ID, login
Ambition Level 2	**e-ID linked with other state-regulated proofs**	
	Extended, secure identification option without media discontinuity	Covid certificate, digital driving license, criminal record, diploma
Ambition Level 3	**Ecosystem of Digital Credentials (a.k.a e-ID ecosystem)**	
	Secure digital processes without media discontinuity	Membership ID, access authorisation, certificates, tickets, immunisation records, etc.

Figure 2

In an Ecosystem of Digital Credentials there are three entities (issuers, verifiers and holders).

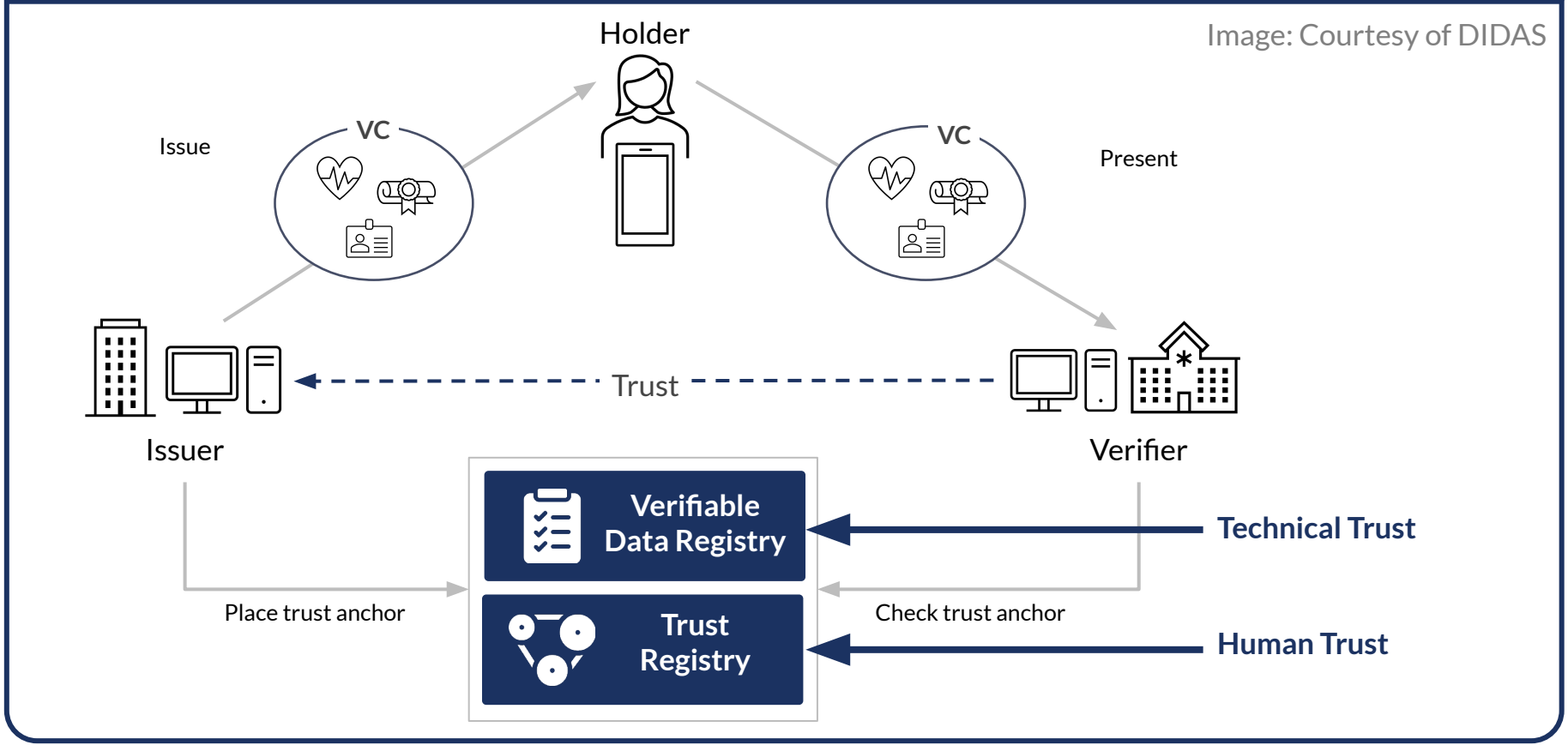


Figure 3

Verifiable credentials offer many benefits beyond current paper-based credentials.

User

- User-controlled
- Reusable
- Instantly-verifiable
- Secure
- Tamper-Proof
- Privacy-preserving
- Digitally-watermarked

Figure 4

Sectoral ecosystems would emerge on a decentral state-operated infrastructure

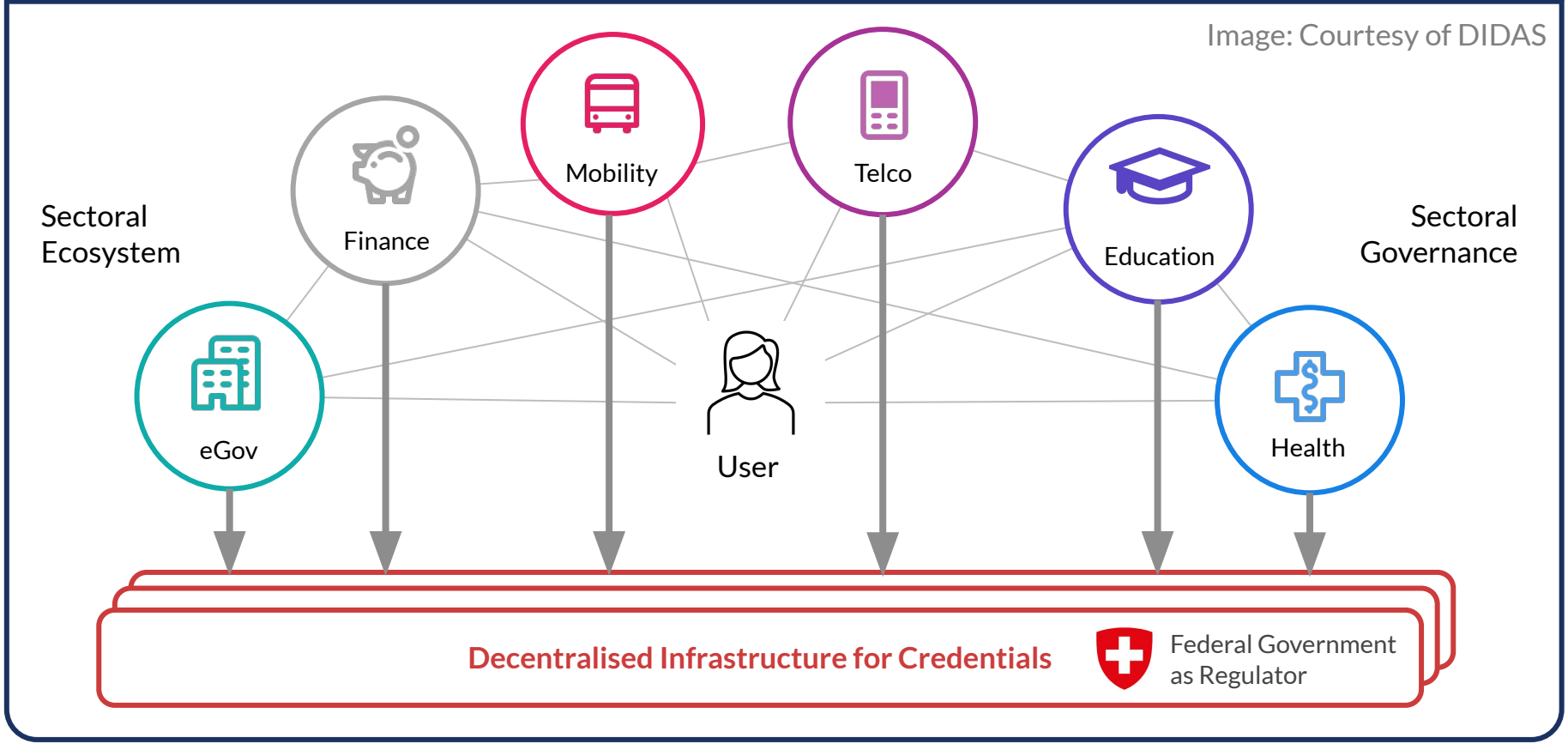


Figure 5

The sectoral ecosystem would reinforce one-another in a move towards a Swiss Digital Trust Ecosystem

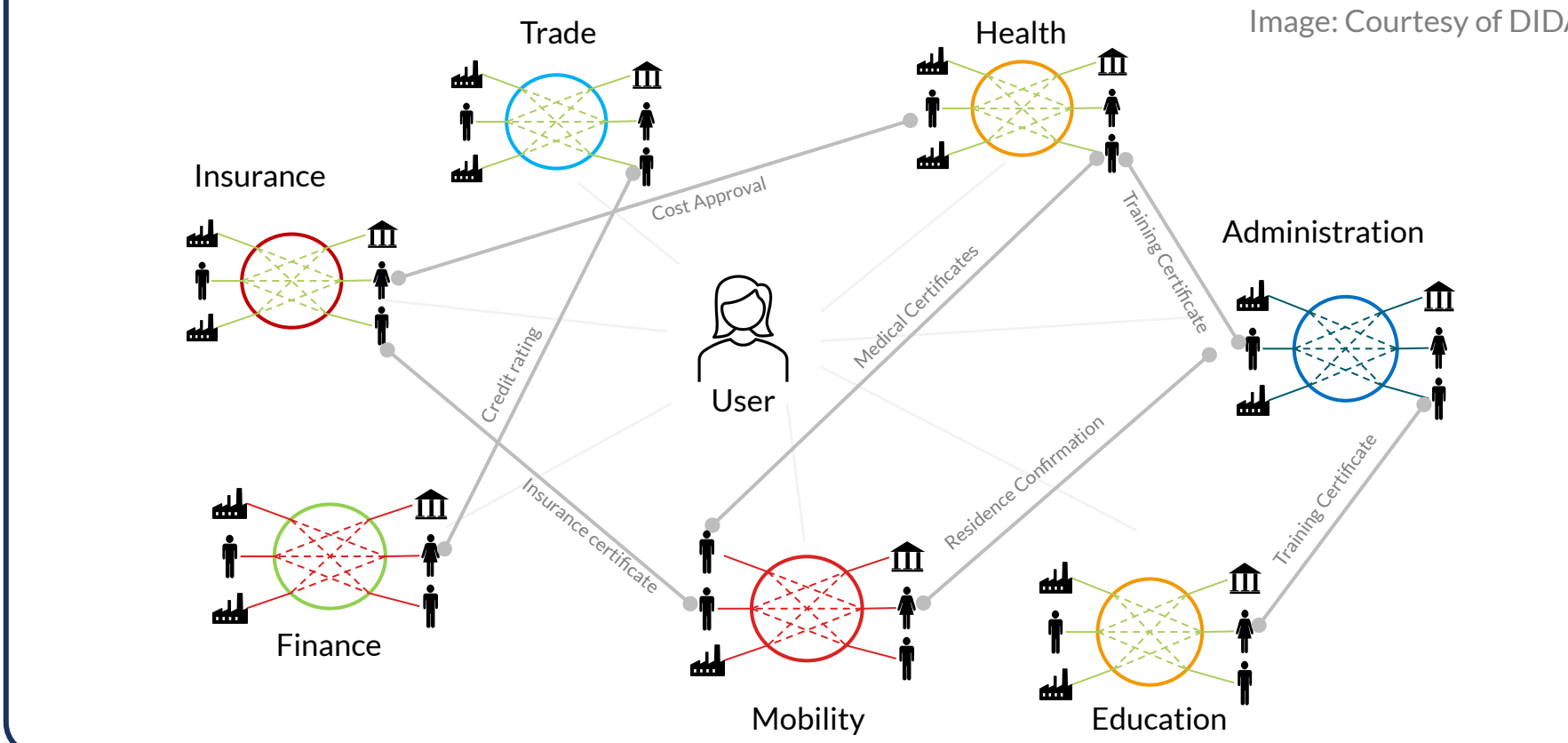


Figure 6

An e-ID ecosystem, following SSI principles, would feature four distinct architectural layers

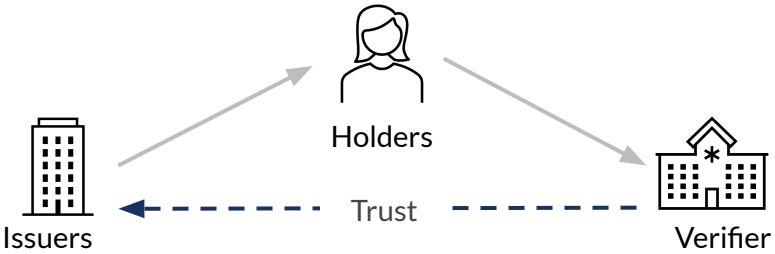
Source: TrustOverIP Foundation

Layer 4 - Application Ecosystem

This layer is about establishing an ecosystem of trust supporting interoperable SSI based transactions between the ecosystems' participants (e.g. Apps, Wallets, Products)

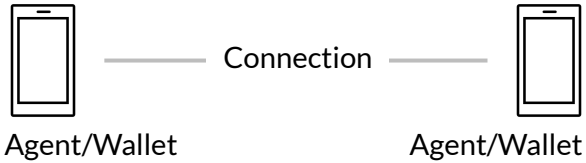
Layer 3 - Data Exchange Protocols

This layer is about establishing human trust on the basis of verifiable credentials and data exchange protocols.



Layer 2 - Secure Communications & Interfaces

This layer is about establishing trust communications between the peers over a DID-to-DID connection (e.g. agents, infrastructure)



Layer 1 - Public Utilities

This layer is about establishing decentralised trust roots. This is where identifiers (DIDs) and public keys are defined, managed and exposed through a verifiable data registry.

Figure 7

Digital Trust Ecosystem requires collaboration between government, private sector, academia & civil society.