digitalswitzerland

Discussion Input

Building a Swiss Digital Trust Ecosystem

Perspectives around an e-ID ecosystem in Switzerland

Published: April 28th, 2022

Table of Contents

Purpose of this Document

The transition to an ecosystem of digital credentials, initiated by the federal government's directional decision, is a generational project that requires input from - and collaboration between - government, the private sector, academia, and civil society. This document is intended to serve as an initial contribution to the ongoing meta-level debate about the development of the e-ID ecosystem in Switzerland. As this field continues to evolve, the document can be understood as an early expert perspective that reflects the views from private sector organisations and academic institutions and will be further refined in future versions.

The document does not constitute a political statement on behalf of digitialswitzerland, nor should it be understood as such. Likewise, the experts' contributions do not imply any political statement on behalf of their respective organisations. The discussion input is intended for all stakeholders in Switzerland, whether from politics, business, academia or administration, who are interested in the ongoing development of the e-ID ecosystem.

About the Authors

This document was jointly written by ten digital identity experts from the private sector and academia. It was produced between January and April 2022 by a working group, called the 'Expert Studio', which was initialised and moderated by digitalswitzerland. All digitalswitzerland members were invited to participate.

The following experts made this discussion input possible through the generous commitment of their time:

Vitus Ammann, Senior Advisor Digital Transformation, SBB CFF FFS
Graeme Entwistle, Emerging Tech Innovator, UBS
Christoph Graf, Programme Manager, SWITCH
Raffael Knecht, Senior Manager/Lawyer, Swisscom
Marius Matter, Member of the Executive Board, ti&m
Frank Michaud, Principal Engineer, Cisco
Stéphane Mingot, Head of Adnovum Incubator, Adnovum
Prof. Dr. Tim Weingärtner, Professor of Blockchain & Smart Contracts, Lucerne University of Applied Sciences and Arts (HSLU)
Prof. Dr. Reinhard Riedl, Professor of E-Government, Berne University of Applied Sciences (BFH)
Andreas Schneider, Chief IT Architect, Allianz Suisse
Jan Friedli, Senior Innovation Manager, digitalswitzerland

About digitalswitzerland

digitalswitzerland is a nationwide, cross-sector initiative that aims to strengthen Switzerland's position as a leading digital nation. Under the umbrella of digitalswitzerland more than 230 organisations, consisting of association members and politically neutral foundation partners, are working together to achieve this goal. digitalswitzerland is the point of contact for all questions relating to digitalisation and is committed to solving a wide range of challenges. Learn more about digitalswitzerland here.

Special thanks go to the Digital Identity and Data Sovereignty Association (DIDAS) for their invaluable contribution to this discussion paper and for generously providing many of the images in this document. We are particularly grateful to Vasily Suvorov, President of DIDAS, for his excellent input.

Executive Summary

Starting Point

In December 2021, the Federal Council took a directional decision that envisions an e-ID ecosystem based on a state-operated infrastructure and in line with the principles of self-sovereign identity (SSI) and the focus on data protection, privacy by design, data minimisation, and decentralised storage. In this context, the e-ID is the main verifiable credential (VC) - to which other VCs can be linked - but nonetheless one VC among many within a digital wallet. There are several national and international efforts relevant for this e-ID ecosystem. See Chapter 1 for details.

The Vision of a Swiss Ecosystem of Digital Credentials

The proposed ecosystem would transpose the current reality of traditional (paper or plastic) credentials to the digital world. Traditional human trust (e.g. trust in reliable issuers of defined credentials in different areas of everyday life) would be complemented by technical trust based on international standards and cryptographic technologies. As far as human trust is concerned, it would be sensible to rely on the same institutions that we trust today in the analogue world. However, to establish technical trust, a national, publicly licensed network with a government-designated supervisory authority would be expedient. The nodes of the network should be distributed across several Swiss organisations, including the government, non-governmental organisations (NGOs), universities, and the private sector. See Chapter 2 for details.

Concrete User Value

Only a level 3 ecosystem, where there are many issuers and verifiers, can offer enough benefits to justify the investment and risks. In other words, opting for ‘small and simple solutions’ carries a much higher risk of failure. A level 3 e-ID ecosystem that follows SSI principles would put the identity holder at the centre and empower them to own their digital identity. For the government and the state, the issuance of various VCs in combination with the e-ID could provide an alternative to the current reliance on in-person authentication and significantly boost digital services in the e-government sector. Finally, the e-ID would offer the basis for innovative services to be built by sectoral ecosystems. See Chapter 3 for details.

Technical Perspective

We recommend implementing the e-ID ecosystem according to SSI principles with the appropriate technology. It would thus consist of three roles (holders, verifiers, issuers) that communicate with each other and verify data using a decentralised registry. Establishing trust in the technologies and standards, as well as in the participants of such an ecosystem will be critical. This can be guaranteed through open standards, robust reference implementations, and a certification process that is instituted by the federal government. In addition, interoperability must be ensured at the three levels of

ambition, between ecosystems in the sector, and in an international perspective, through the use of common standards by all stakeholders. To gain confidence and insights, it would be useful to set up a sandbox with representative use cases to validate the standards and establish a reference implementation. With this approach, we can lay the foundation for productive use of the technology and governance framework. See Chapter 4 for details.

Governance Perspective

In the analogue world, we use the well-established Swiss ID card for various identification processes and leverage the existing human trust in the state governance of the processes around the ID card. According to Level 3, an e-ID ecosystem should transfer this existing trust to the digital world by having - wherever possible - the same entities that already ensure human trust in the ID card ecosystem take on the same role in the ecosystem of digital credentials (EDC). This could be accomplished by mirroring the e-ID process to that of the ID card and giving existing trust operators (e.g. the commercial register) a corresponding role in the EDC (e.g. issuing VCs with information from the commercial register). Many sectoral use cases will rely on such existing trust services. See Chapter 5 for details.

Legal Perspective

Creating a reliable digital trust ecosystem, where secure identities form the basis for legal proof fills an important gap, as the lack of trust-building elements in digital transactions is the biggest barrier to digitisation today. Addressing this shortcoming will create a solid breeding ground for the digital economy and for high-quality e-government. From a legal perspective, it would be useful to create a legal framework that is in line with international e-ID solutions, especially those of the EU. See Chapter 6 for details.

Usability Perspective

An e-ID ecosystem in line with SSI principles implies that the responsibility for managing the digital wallet and its VCs is transferred to the user. This brings significant advantages (e.g. data ownership), but also requires considerable secondary efforts (e.g. awareness campaigns). The digital wallet as the central interface to the e-ID and VCs is particularly important and should be as intuitive as possible. The issuing and revoking of VCs must thus be simple, fast, and straightforward. In addition, societal diversity needs to be considered when discussing and implementing the e-ID, the associated VCs, and the digital wallet. In the spirit of digital inclusion, all citizens must be actively supported in understanding and using the new technologies (e.g. through training). See Chapter 7 for details.

Economic Perspective

The opportunity cost of the unresolved trust problem as an obstacle to digital transformation is very high. In building an EDC, however, we face a kind of chicken-and-egg problem involving three actors (holders, verifiers, issuers). In this context, a Level 3 e-ID ecosystem has the greatest chance to succeed. To enable adoption, the cost of issuing the e-ID should be equal or less than the cost of issuing the physical ID card it digitally represents. Further, the identification process via e-ID should therefore be free of charge for both consumers and organisations. In general, building an ecosystem can neither be fully planned in advance nor can it be fully implemented ad hoc. See Chapter 8 for details.

Possible Roadmap

The starting point for the building of the e-ID ecosystem will be the issuance of the e-ID itself, together with e-ID enabled digital signatures. The Swiss government has the political mandate for this implementation. This will kick off two parallel work streams. One will focus on developing demonstrators that show potential use cases in a sandbox setting, the other on designing and building infrastructure and governance. For example, e-government services could start accepting government-issued VCs in combination with the e-ID. The ecosystem, in turn, could issue VCs in combination with the e-ID in cases where the short- to medium-term economic benefits are obvious and/or for instances where broad stakeholder commitment can be achieved through regulatory means or through existing offerings. See Chapter 9 for details.

Glossary

Agent	In the SSI context: all issuers, verifiers, and holders are agents that communicate with each other using the communication protocols specified for the decentralised identity network.
Attribute	Single data point, e.g. first name or date of birth. Sometimes referred to as 'claim' in the SSI context.
Bug bounty program	A bug bounty program, also called a Vulnerability Rewards Program (VRP), is a crowdsourcing initiative that rewards individuals for discovering and reporting software bugs.
Credentials	Dataset consisting of one or more attributes.
Data minimisation	Two aspects are subsumed under the term data minimisation: The reduction to the necessary minimum of attributes when transmitting data to third parties and the avoidance of unnecessary data flow and associated marginal data.
Decentralised data storage	Data is not kept in a single, central repository, but is distributed across a network of storage systems or offloaded to end-user devices.
Decentralised identity	An electronic identity that is not managed by a central system and can only be used by way of this system, but is instead stored on the user's smartphone, for example, and can be used directly via such a device.
Decentralised identifiers (DIDs)	A new type of identifier that enables verifiable, decentralised digital identity. A DID refers to any subject (e.g., a person, organisation, thing, data model, abstract entity, etc.) as determined by the controller of the DID.
Digital trust infrastructure	A set of regulations, processes, concepts, and infrastructure elements that ensure trust in and fidelity to digital processes and that are accepted and used by a broad public.
Ecosystem of digital credentials (EDC)	A set of infrastructures, public and private participants, and governing rules that enable the issuance and revocation, holding, transmission, and verification of digital credentials of any type and for any purpose. (see also e-ID-ecosystem).
e-ID	e-ID stands for governmental electronic identity - a type of digital proof with which users can prove their own identity.
e-ID ecosystem	Interaction of a multitude of actors (public and private) with different uses and offerings that take place with and around the e-ID and on the basis of a shared digital trust infrastructure. 'e-ID ecosystem' is the Swiss terminology for the much broader term 'Ecosystem of digital credentials' (see Ecosystem of digital credentials).
Trust ecosystem	A set of regulations, processes, concepts, and infrastructure elements that ensure trust in digital processes and their process fidelity and that are accepted and used by a broad public.
eIDAS regulation	eIDAS stands for Electronic Identification, Authentication and Trust Services' and is an EU regulation establishing uniform rules for electronic identification and electronic trust services.

ESSIF	The European self-sovereign identity framework (ESSIF) is part of the European blockchain service infrastructure (EBSI). The EBSI is a joint initiative of the European Commission and the European blockchain partnership (EBP) to deliver EU-wide cross-border public services using blockchain technology.
Holder	In the context of SSI and PKI, the holder stands for the owner of a wallet that contains verifiable credentials.
Identity hub backup	Electronic backup facility of verifiable credentials that provides the data for recovery and enables data transfer to other devices. This can be self-managed by users on their own hardware or provided by a provider with cloud functionality.
Identity Management	The processes and policies for managing the lifecycle and value, type, and optional metadata of attributes in identities known in a given domain (as per ISO/IEC 24760-1).
Identity	A set of attributes related to an entity, and an attribute as a characteristic or property of an entity (as per ISO/IEC 24760-1).
Identity provider (IdP)	The technical system component where a login is carried out in order to subsequently 'guarantee' the identity of a user. In a broader sense, an identity document or a wallet can also be an identity provider.
Institutional agent	Term in the SSI context, introduced by the German SSI pilot project IDunion: Software application for issuing and verifying verifiable credentials.
Issuer	Institutions, organisations, and also private individuals who issue verifiable credentials and hand them over to the user.
Legal entity identifier (LEI)	A unique global identifier for legal entities participating in financial transactions. It is also referred to as the LEI code or LEI number and is intended to help identify legal entities in a globally accessible database. The Global legal entity identifier foundation (GLEIF) is tasked with supporting the implementation and use of the Legal entity identifier (LEI).
Level of ambition	Term from the revision of the eIDAS regulation to clarify the scope of the use of an e-ID infrastructure.
Minimum Viable Product	A minimum viable product is a version of a product that has just enough features to be used by early adopters who can then provide feedback for future product development.
Node	Storage node in a distributed storage network (distributed ledger, DLT).
Peer-to-peer communication	In the context of SSI, describes the data flow between issuer and holder or holder and verifier.
Privacy by design	Design principles according to which data protection and in particular data minimisation are ensured by the conceptual design.
Public key directory (PKD)	Central register in which the public keys of issuers of proofs are stored. In hierarchical PKIs with precisely one trust anchor, no PKD is needed.
Public key infrastructure (PKI)	Overall system of a trust network built on the basis of asymmetric encryption technology.

Public key cryptography	Asymmetric encryption technique in which one key is made public and the other key must remain private.
Quadruple and quintuple innovation helix framework	A framework that describes the interactions between university, industry, government, and the public in a knowledge economy. It was developed by Henry Etzkowitz and Loet Leydesdorff and is used in innovation economics and knowledge theories.
Registry (Verifiable Data Registry (VDR) & Trust Registry)	In the SSI context: Term relating to publicly readable storage with the necessary cryptographic evidence for the validity verification of verifiable credentials. There are two different kinds of registries: Verifiable Data Registry (also known as DID registry): a registry accessible via the Internet that contains all essential data and metadata allowing the verification of verifiable credentials. It includes, but is not limited to, the DIDs (see decentralised Identifiers), the verification methods, and the issuer's public cryptographic key. Verifiable data registries can be, for example, distributed ledgers. Important: the VDR does not store verifiable credentials; these are stored in the wallet. Trust Registries: registries accessible via the Internet that contain a list of trusted issuers and, where applicable, verifiers, that are administered by the governing authority of the sector.
Relying party (RP)	Analogous to verifier, term in the IdP context: System participants making use of the e-ID ecosystem to verify identity credentials and utilise the personal data represented by the e-ID.
Sector Ecosystems	Sector-oriented ecosystems around topics and/or industries: health, education, government, finance, insurance, mobility.
Self-Sovereign Identity (SSI)	A set of principles centred on data protection and users, which in recent years has led to a derived technological approach to electronic identities. In the context of SSI, users themselves are responsible for managing their own verifiable credentials, issued by issuers and thus trustworthy.
Trust Over IP (ToIP) framework	Guidelines for defining decision-making levels on governance and technology implementation issues, developed by working groups of the Trust Over IP Foundation.
Verifiable Credentials (VC)	Dataset consisting of one or more attributes, signed as ‘verified’ by the issuer and then handed over to the user. The issuer, the date of issue, and the cryptographic proofs are part of a verifiable credential in addition to the actual data.
Verifier	Analogous to the relying party, the term in the SSI context: System participants that make use of the e-ID ecosystem to verify credentials and utilise the data presented by the users.
Wallet	A software application, often designed as a smartphone app, which stores verifiable credentials and ensures communication with issuers and verifiers. The wallet, therein, acts primarily only as storage. The agent is the active component (see Agent).
Zero Knowledge Proof (ZKP)	A method by which one party can prove to another party that a given statement is true, while the prover avoids conveying any information other than the fact that the statement is indeed true.

Chapter 1: Starting Point

1.1 Context

In September 2019, the Swiss parliament passed the Federal Act on Electronic Identification Services (e-ID Act) by a clear majority. Shortly thereafter, a referendum was successfully called against the e-ID Act. It was clearly rejected in March 2021. Following the rejection, the federal council instructed the Federal Department of Justice and Police (FDJP) to swiftly work out a solution in cooperation with the Federal Chancellery (FC) and the Federal Department of Finance (FDF). On this basis, the FDJP conducted a public consultation from September 2 to October 14, 2021. digitalswitzerland was invited to provide its perspective. The primary purpose of the public consultation was to determine the scope of future e-ID use ("levels of ambition") and accordingly the scope of the ecosystem. Three levels of ambition were presented in the process. In a second step, three technological implementation options were presented as a basis for discussion in the public consultation: Self-sovereign identity, public key infrastructure, and central governmental identity provider. A detailed presentation of the ambition levels and the associated technological implementation options can be found in the "Discussion paper on the target vision for an e-ID".

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.

On behalf of its members, digitalswitzerland submitted a written statement on October 13th to advocate for ambition level 3 (ecosystem of digital credentials), at the same time emphasising the importance of data protection and sovereignty, well-aligned governance principles, and international connectivity. The full written statement can be found here.

1.2. Directional Decision

60 written comments were received from 21 organisations, 16 cantons, 16 companies, 4 political parties, and 3 higher education institutions. According to the aggregated analysis by the FDJP in

November 2021, ambition level 3 is named as the final target by almost all participants who explicitly commented on the ambition level. A majority of the participants also see the Self-sovereign identity (SSI) technology approach as the best possible option to implement the required value propositions and functions. On this basis, the federal council communicated the principles for the design of a future state e-ID in a press release on December 17, 2021. They are:

> *"The users of the e-ID should have the greatest possible control over their data (self-sovereign identity). Data protection should be ensured, among other things, by the system itself (privacy by design), but also by minimising the necessary data flows (principle of data minimisation) and decentralised data storage. The e-ID should be based on a state-operated infrastructure. It could be available to government and private entities for issuing various digital credentials (e-ID ecosystem)."*

With this guidance, the federal council is meeting the demands of various parliamentary initiatives. The directional decision points out that the e-ID, based on a state-operated infrastructure, is the most important verifiable credential (VC), but still one VC among many within the e-ID ecosystem (see Chapter 2). The consultation procedure for the new law (germ. Vernehmlassung) will begin in mid-2022; the federal council will then prepare and adopt a dispatch by autumn 2023 (germ. Verabschiedung der Botschaft). In order to account for the rapidly-evolving nature of technology, the law will be formulated in a technology-neutral way. As part of the preparation of the dispatch, the FDJP and the federal council are still examining various points such as the issuing procedure and the scope of operation of the e-ID infrastructure by the state.

In the federal council's directional decision two central points were further specified: First, the e-ID ecosystem should be built in stages (germ: 'schrittweise'). Second, the federal government outlined its intention to launch three pilot projects.

Three Federal Government Pilot Projects

Pilot Project '**Digital Driver's Licence**', led by the Federal Roads Office (FEDRO) and the Association of Swiss Road Traffic Offices (asa) with a focus on connecting specialist applications, credential content and testing.

Pilot Project '**Proof of Concept ePerso** (germ. 'Bundespersonalausweis'), led by the Federal Personnel Office with a focus on security aspects and logins.

Pilot Project '**Base Infrastructure**' (germ. 'Basis-Infrastruktur'), led by the Federal Office of Information Technology, Systems and Telecommunication (FOITT) with a focus on the shared infrastructure and aspects revolving around wallet, registry and communication.

In parallel, the federal government's e-ID project team has established a 'Governance sounding board' as well as an 'Open source community' for external stakeholder participation. Both take the form of community-facilitated GitHub forums open to the public.

1.3. Efforts in Switzerland

The Swiss market for an ecosystem of digital credentials is gradually maturing with several promising initiatives and use cases. Such efforts provide a unique opportunity to learn in a real-world working context that is driven by the private sector and has the potential to inspire other projects. While there exists a multitude of such use cases and initiatives, we highlight here three of the most mature efforts in the Swiss market.

Strategic partnership between Orell Füssli and Swisscom
On January 4, 2022, Orell Füssli and Swisscom announced a strategic partnership, to offer trusted, forgery-proof, and smart digital certificates to citizens, businesses, and public authorities. These will be retrievable in real-time via smartphone, according to the press release. These digital certificates can be verifiably integrated into business processes to enable new and more efficient user interactions. These include age verification when purchasing age-restricted products or at entry checks, digitally verifiable applications, and the combination with legally valid digital signatures as a digital expression of will. The solutions developed, which are to be made available within the next 12 months, are based on the principles of privacy by design, data economy, and decentralised data storage.

SSI-initiative, a joint project of the canton of Aargau, Adnovum, cardossier and SwissSign
On January 12, 2022, an initiative was announced that aims at building an exemplary self-sovereign identity (SSI) ecosystem. The intent is to lay the groundwork for exploring aspects of technology, user experience, added value, and compliance. To highlight the issuance and use of digital credentials in the form of SSI verifiable credentials (VC), the exemplary SSI ecosystem consists of three use cases. First, the issuance of a basic identity on the grounds of a SwissID. Second, building on this, a certificate of residence (germ. 'Wohnsitzbescheinigung)' is issued on the eGov portal of the canton of Aargau. Third, the registration of a vehicle on the cardossier platform, which stores all relevant information about a vehicle's history, with the policyholder's identity and certificate of residence serving as verifiable credentials. The initiative has already led to numerous insights and is open to interested players looking to enrich the ecosystem with use cases.

A decentral identity for eGov services offered by Zug, ti&m, HSLU, and uPORT
In the summer of 2017, the City of Zug launched a pilot programme to register resident IDs on the public Ethereum blockchain. This was one of the world's first live implementations of a government-issued self-sovereign identity project on the Ethereum blockchain. The Institute for Financial Services Zug of the Lucerne University of Applied Sciences and Arts, the companies Consensys-uPort and ti&m, as well as the IT department of the city of Zug were involved in the development and implementation. The pilot program has enabled Zug citizens to manage their personal identity data which is stored neither centrally nor on the Internet but encrypted on their own cell phones. Without the user's consent, the data on the cell phone remains locked. In 2018, Zug citizens were able to participate in the first blockchain-based ballot. Since 2020, the IT department of the city of Zug has been developing the eZug app to enable residents to use municipal government services via a digital channel, such as the issuance of a certificate of origin (germ. 'Heimatausweis').

The three aforementioned projects represent the first concrete steps towards building an ecosystem of digital credentials. While this is only a small sample of the overall activities in this area, these initiatives and use cases clarify several aspects:

1. These use cases follow an ecosystem approach with public and private sector organisations that need to work together to deliver value to the user.
2. The broad range of applications speaks to the versatility of the SSI framework and the importance of the sectoral ecosystem (see Chapter 2).
3. The value proposition delivered by the SSI framework can be interpreted differently depending on the respective end-user (e.g. increasing privacy or reducing the administrative burden).
4. There is a wide variation in technical design (e.g. blockchain or no blockchain).

In general, it should be noted that many of the SSI initiatives in Switzerland are still in an experimental phase and consequently have only a limited number of active users. In order to scale up such initiatives to nationwide solutions, it is imperative to avoid fragmentation of the SSI landscape and to find common ground.

Several organisations are taking a leading role alongside digitalswitzerland in the search for such common ground. These include the Digital Identity and Data Sovereignty Association (DIDAS), a non-profit organisation based in the Canton of Zug. The primary goal of DIDAS is to establish and promote Switzerland as a leading ecosystem in the development and introduction of technologies, services and products for the protection of privacy that preserve and use digital identity and electronically verifiable data. In addition, many IT service providers have demonstrated their expertise and commitment to the expansion of the Swiss ecosystem. Among them are Adnovum, Cisco, Swisscom, Switch, ti&m, and others.

1.4. International Development

The need for trust in digital interactions does not stop at national borders. Many other international developments are impacting the Swiss landscape for an ecosystem of digital credentials. In addition to the international legal context (see Chapter 6), several notable international developments exist:

The World Wide Web Consortium

The current regulatory uncertainty has resulted in the formation of several industry-led consortia that are working together to establish standards and/or guidelines to support the development of SSI initiatives at an international level. Among the most influential of these efforts is the World Wide Web Consortium (W3C). The W3C is an international community with over 450 members working together to develop Web standards. Through its verifiable credentials working group, it has produced a number of foundational documents, including the widely accepted Verifiable Credentials Data Model V1.1.

The Hyperledger Foundation

In parallel, the Hyperledger Foundation, which is part of the larger Linux Foundation, hosts a number of enterprise-grade blockchain software projects, conceived and built by the developer community. Here two collaborative projects are of particular note. *Hyperledger Aries* provides a shared, reusable and interoperable toolkit for initiatives and solutions focused on creating, transmitting, and storing VCs, while *Hyperledger Indy* provides tools, libraries, and reusable components for digital identities rooted in blockchains that are highly interoperable.

The Trust Over IP Foundation

Another international effort impacting the SSI landscape is the Trust over IP (ToIP) Foundation, which was launched in May 2020 and already counts over 300 member organisations at the time of writing. Its stated goal is to create and converge an interoperable architecture for decentralised digital trust at the intersection of digital identity, verifiable credentials, and blockchain technology. To achieve this, ToIP has launched several collaborative working groups. To date, they have produced various foundational documents, design principles, and specifications for the digital trust landscape that are widely supported by the expert community.

IDunion

Building on these collaborative standards, the IDunion, an ecosystem of public and private parties, has begun developing and operating a basic infrastructure to enable the issuance and verification of digital credentials. The vision is to build and operate a decentralised network to link and secure the identities of individuals, legal entities, and things, in compliance with the relevant legal requirements in Europe (e.g. the General Data Protection Regulation (GDPR) or the Regulation on electronic identification and trust services (eIDAS Regulation)). The IDunion concept for decentralised and self-sovereign identities complies with the global standards of the W3C and the ToIP Foundation.

ISO Technical Committees

Several specific working groups of the International organisation for standardisation (ISO) are also noteworthy, including the technical committees 'Security, privacy and identity for Blockchain and distributed ledger technologies (DLT)' (TC307/JWG4), 'Overview of existing DLT systems for identity management' (TR23249), and 'Overview of trust anchors for DLT-based identity management' (TR23644).

The European Self-Sovereign Identity Framework

Another important development is the European self-sovereign identity framework (ESSIF), which is part of the European Blockchain service infrastructure (EBSI).

All these international consortia, ecosystems, and standards have practical consequences for Switzerland. If we wish to preserve the option of international interoperability and connectivity to emerging ecosystems (e.g. IDunion), we should be mindful of these standards and consider joining these efforts.

Private Sector Initiatives

At an international level there are other important developments that revolve around the initiatives launched by technology and electronics companies. Other than physical wallets, SSI initiatives focus on digital wallets within mobile phones. Corresponding initiatives have been launched by several companies. This is particularly evident in countries with more tech-friendly legal frameworks, such as the US.

Apple, for instance, has announced that some of its users can now add driver's licences and ID cards to their Apple wallets. The U.S. states of Arizona, Connecticut, Georgia, Iowa, Kentucky, Maryland, Oklahoma, and Utah are among the first to participate in pilots. In addition, selected U.S. airports will be the first to allow users to get through security using the digital ID stored in their wallet app. *Google* also is widely believed to be pushing its own initiatives to link driver's licences and passports to Google Pay, but no official statements have yet been released at the time of writing. The tech-friendly regulatory framework and their financial muscle give these companies the ability to quickly develop and launch services. In some cases, they may move faster than legislative developments.

Meanwhile, *Microsoft* maintains that if the EDC is to grow, the standards, technical components, and code must be open-source and accessible to all. Microsoft, therefore, focuses on working with members of the Decentralised identity foundation (DIF), the W3C Credentials Community Group, and the wider identity community.

In Germany, Samsung has partnered with the Federal Ministry of the Interior, of Construction and Home Affairs, the Federal Office for Information Security, Bundesdruckerei, Deutsche Telekom Security, Governikus as part of the OPTIMOS 2.0 project. It makes it possible to securely store the identification data stored in the chips of identity documents, such as the ID card, on compatible smartphones. While the first compatible mobile phone is from Samsung, the underlying open ecosystem is connectable for different identity service providers.

There are, quite obviously, still more initiatives at an international level, but a complete overview is beyond the scope of this discussion input. The important point here is that the initiatives of technology and electronics companies must be taken into account, as they have a considerable influence on the development of the SSI landscape in Switzerland.

.

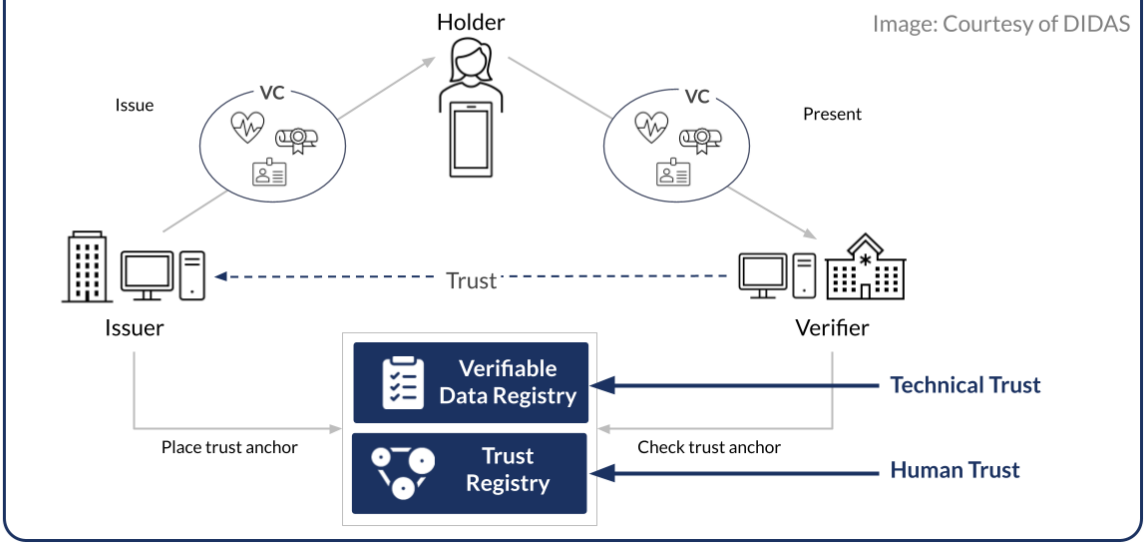
Chapter 2: Vision of a Swiss Ecosystem of Digital Credentials

2.1. Overview

The diagram shows the key players in the ecosystem of digital credentials. By way of example, an issuer (e.g. a university) might issue a credential (e.g. a degree) to a holder (e.g. the successful graduate), who can then present this credential to a verifier (e.g. a prospective employer). The latter then verifies that the degree comes from a properly accredited university via the trust registry, which is a list of accredited issuers of credentials. Only the holder is in possession of the degree certificate and can present it to any number of potential employers without the university's knowledge or involvement in the process, as is the case with today's physical credentials. The authenticity and validity of the presented credentials can be verified via the cryptographic fingerprint of the credentials stored (without any reference to the content of the VC) in the verifiable data registry. Many types of credentials can be issued and submitted this way. In the following subsections, we elaborate on and discuss these various components.

Figure 2

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



2.2 Verifiable Credential

A *credential* is an assertion or proof of something about someone. In our example above, the degree certificate is proof that a certain level of education has been achieved at a particular university. Credentials are issued by an issuing authority (see 2.4) which may be a public or private body. The issuer is, in turn, certified as such by either an appropriate government agency or a sector-specific authority. This certification confirms that the issuer has the right to issue certain credentials, so that trust is firmly rooted.

A *verifiable credential (VC)* is a digital representation of what may currently be a paper-based credential (ID card, driver's licence, health pass, diploma, membership card, etc.). It can be verified by cryptographic means as having been issued by a specific issuer without the issuer being involved. The e-ID is a VC issued by the government. It is one of many VCs, but arguably the most important. When issued, a VC may be tied to the e-ID, which is called the subject of the VC.

It is possible for a credential to expire at a predetermined time, to be deleted by the holder, or be revoked by the issuer. For example, our student's degree might be revoked by the university if he or she is found guilty of plagiarism. It will be part of the verification procedure conducted by the verifier, to determine whether or not an otherwise valid credential has been revoked.

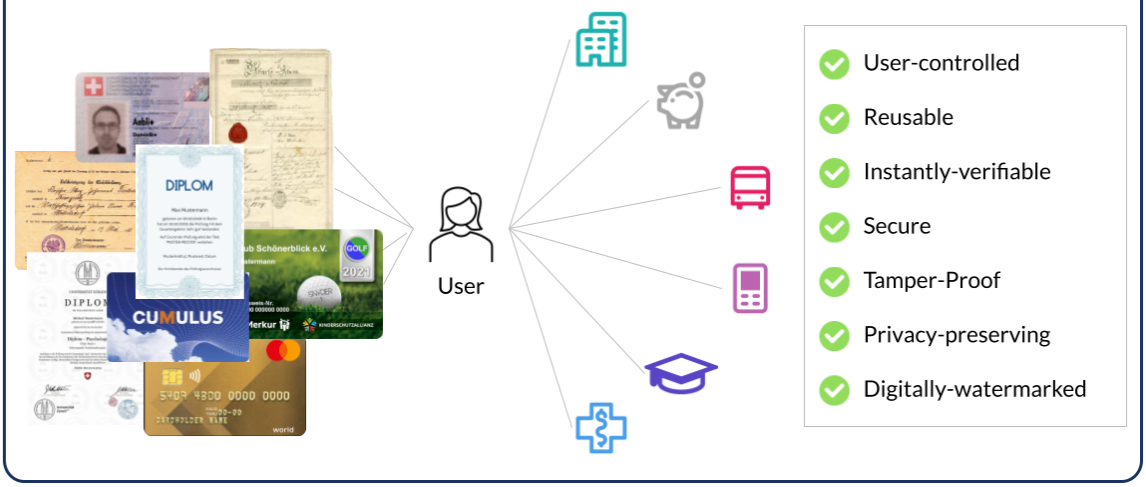
The e-ID ecosystem, made up of many VCs, is fundamentally inclusive and open. There will be points of connection between existing solutions and the new e-ID ecosystem. It is important to draw a clear distinction between current private ID solutions (e.g. SwissID) and the e-ID (i.e. the digital representation of the ID card). Pre-existing private IDs can be issued and used as VCs in the new ecosystem. However, none of them could become the e-ID. The issuance and control of the e-ID as a VC lies solely with the government.

2.3. Holder with Wallet

The holders are the sole owners of all credentials issued to them. Just as they used to keep paper or card-based credentials in physical wallets or files, they now store their digital credentials in a wallet.

Figure 3

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



The wallet is an application that runs on a computing device, such as a cell phone (for technical details, see Chapter 4). It performs transactions solely on the holders' behalf, provided that they have given consent.

In case a verifier requests proof of a specific credential claim and the holder gives consent, the digital wallet sends this proof with the required information only. This gives the holder full control over whom they share the credential proof with. Issuers never know when or where any of the credentials they have issued are being presented. For example, in a transaction that requires proof of age, such as the purchase of a bottle of wine, the user might decide to only provide proof that they are "over 18", while refraining from sharing other information, such as their exact age.

Wallets that 'store' all the VCs may be offered to holders by the government or by private organisations as stand-alone applications or as part of a broader service package. We suggest that the government set standards and rules for security, privacy and data protection so that holders can have trust in their agents. Usability issues are addressed in Chapter 9.

2.4. Issuer

The issuer creates verifiable credentials at the request of an individual, confirming certain attributes of that person. These credentials are forwarded to the person, henceforth called the holder, who has then full control over them. The issuer has no way of tracking the use of these credentials. The issuer can be a public or private person or organisation certified to issue credentials for a specified type of attribute. An example would be a university certified to issue bachelor's degrees, master's degrees, PhDs, cas, das, and emba degrees. This creates a *chain of trust* that should be rooted in government and involves the issuers of analogous degrees, namely universities. In the above example, universities of all types are the natural institutions to issue digital credentials for academic degrees.

2.5. Verifier

Anyone and anything can act as a verifier of credentials if - *and only if* - the holder is willing to submit them. An example of a verifier might be a prospective employer requesting proof of academic qualifications. The verifier communicates with the holder via the wallet, first to obtain permission to establish a secure connection, and then to ask for the required credentials or specific claims contained in a credential. The credential contains all the necessary information to allow the verifier to ascertain the accuracy and validity of the credential. As mentioned above, there is no communication between the verifier and the issuer at any time.

2.6. Registry / Trust Infrastructure

Trust is a central issue when it comes to representing and verifying identities. In the trust triangle (issuer-holder-verifier) the verifier can check the authenticity and validity of a verifiable credential presented to him. The verifier is able to trust the issuing party (the issuer), as evidenced by the trust registry. This trust infrastructure is based on secure, resilient, and privacy-preserving decentralised registries which use cryptographic technologies. Trust is ensured without the need for direct communication between verifier and issuer.

2.6.1 Verifiable Data Registry

It is very important that the verifiable data registry does not store identity data, but only cryptographic information (DID, public keys, revocation information, no credential content) and therefore supports principles of privacy by design. This cryptographic information is provided by the issuers. The registry must support not only credential issuance and verification, but also revocation. A distributed implementation guarantees high availability and resilience to attacks on or failures of single nodes.

2.6.2 Trust Registry

The trust registry stores information about the participating parties (mainly issuers) so that anyone can verify that an issuer is authorised to issue and revoke credentials of a particular type. It reflects human trust at the appropriate level in the system.

2.6.3 Governance of Trust Infrastructure

Governance of this trust infrastructure, consisting of both registries, is critical. We suggest that the government, in collaboration with the private sector, academia, and civil society, develop a formal "requirement profile" (germ. “Anforderungsprofil”). In this, we see the value of a national, publicly accredited network where the supervisory authority is appointed by the government. This government supervision is an expression of the trust and values Switzerland stands for. In accordance with the principles of decentralisation, the network should be spread across several Swiss organisations (government, NGOs, universities, larger companies, etc.) to ensure a high degree of distribution. One option for implementation would be through distributed ledger technology (DLT) to take advantage of features such as immutability, transparency and distribution. The government should ensure adequate distribution and be guided by the principles of performance, security and efficiency. Nevertheless, a permissioned character with government supervision should be guaranteed. This means that only approved stakeholders listed in the trust registry can write to the verifiable data registry. Furthermore, even though the network is Swiss, international interoperability must be guaranteed at all times. This is achieved by basing it on international standards, such as the SSI standards.

2.7. (Sub-)Ecosystems / Sectors within the e-ID-Ecosystem

We are used to keeping all kinds of credentials in our physical wallets and files, from ID and membership cards to health-related documents, licences, diplomas and much more. In an e-ID ecosystem, all of these credentials are typically managed within a specific sector, also known as a sector-EDC. In the conceptual model published by the Trust over IP foundation (ToIP) the term ‘ecosystem’ is normally used to refer to a specific sector (e.g. health ecosystem).

Clear rules for issuing and validating credentials in each sector have been established for the analogue world. All these rules only need to be adapted to the new possibility of issuing the credentials in a verifiable digital form. The same authorities that set the rules in their respective

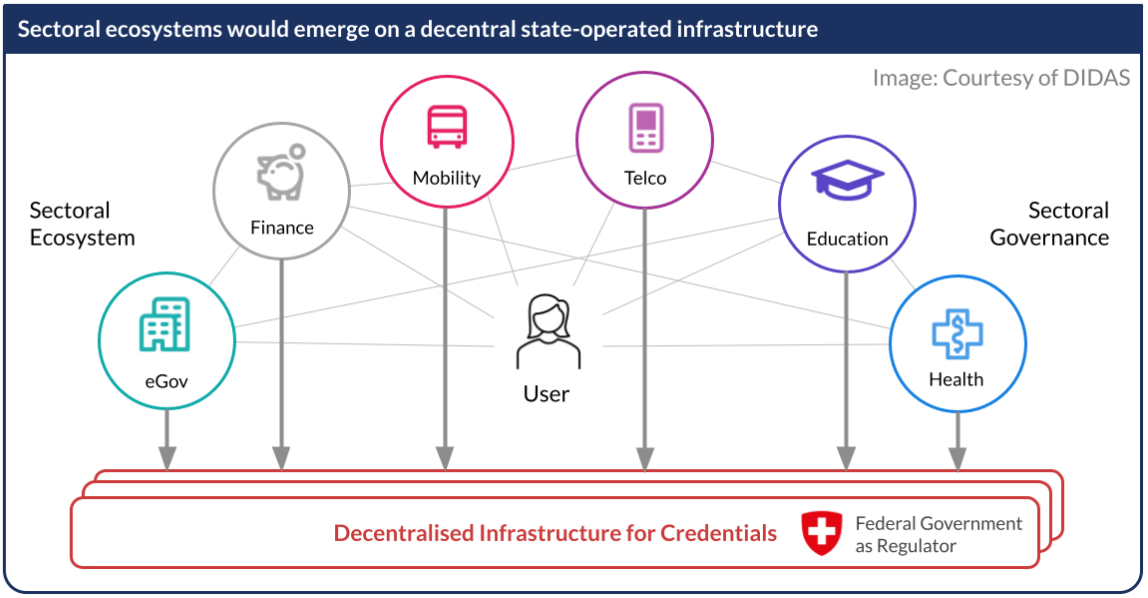
sectors must do so for the definition and issuance of verifiable credentials. They also need to ensure international interoperability within their sector.

One of these sectors is the area of e-government, where official credentials such as an e-ID and all kinds of licences are issued. Here, too, the relevant regulations and authorities are already well defined for physical credentials such as ID cards or a driver's licence. They will need to be adapted for use within an ecosystem of digital credentials (aka e-ID ecosystem).

Another task of the federal government will be to define standards, rules and organisation of the basic infrastructure, such as the verifiable data registry and the technical standards for the various applications for issuing, holding and verifying digital credentials (see Chapter 4). The federal government has already launched pilot projects in these areas, including the federal ID card and the base infrastructure (see Chapter 1).

Figure 4

Sectoral ecosystems would emerge on a decentral state-operated infrastructure



In order to maximise the adoption, reach and efficiency of an e-ID ecosystem, all sectors must be able to use the same trust network for issuing and verifying their sector-specific credential types as early as possible. Most credentials will be used across multiple sectors as illustrated by the following examples:

Public Sector

Government agencies act as both issuers and verifiers of VCs: All official documents and certificates issued by municipal and cantonal authorities to private individuals can be issued in digital form. This means that driver's licences, extracts from various registries (commercial registry, land registry, criminal records registry, debt enforcement registry, etc.) and certificates based on registries such as the civil status registry can be issued as digital credentials by the same agencies issuing corresponding analogue certificates today. The digital counterpart of the passport and the identity card is the e-ID, the electronic identity.

In addition to its role as an issuer, the government also acts as a verifier of documents in its interaction with citizens and businesses. They have the option, but not the obligation, to submit digital credentials that are issued either by government agencies or by other institutions. In the case of a tax declaration, all types of documents that citizens are required to submit could be issued as digital credentials by employers, banks, mobility service providers, insurance companies, etc. Digital credentials can be used to prove income as well as deductible expenses. The same is true for most mandatory government services, whether activities that are mandatory for citizens - such as the registration of a change of residence - or activities requested by citizens, such as changing entries in the land register.

Health Sector

In the health sector, the information contained in the analogue health insurance card can be covered by a health insurance credential issued by health insurance companies, which can also issue cost commitment statements. These credentials are then verified by health service providers to clarify in a trusted way who will cover the costs incurred.

In addition, all types of documents certifying health information, such as vaccination or recovery certificates, can be issued as verifiable credentials. In this regard, government-approved health care providers issue the certificates to individuals and stakeholders wishing to ascertain a person's health status and act as verifiers. These certificates may be used in immigration portals, registration portals (e.g. for hospital admission), or in booking portals (e.g. when a Covid-certificate is required to attend a theatre performance) to reduce the burden of control for both parties. Since it is a chain of trust that needs to be verified, rather than individual credentials, it is easy to revoke credentials if an issuer creates fake certificates, e.g. for vaccinations. This is especially important when the issuer is unwilling to revoke forged health certificates. In such a case, the authority of the issuer to issue certain certificates is revoked.

Education Sector

There is a wide range of applications in education. Membership cards (e.g. student ID cards or the Edulog ID card in schools, library cards, etc.), certificates of attendance, and all kinds of diplomas can be issued as verifiable credentials. The issuers, in this case, are schools, universities and other educational institutions. These organisations may also act as verifiers - e.g. for enrolment in a school or university, or to ensure access to library services - but in addition, many other organisations may also act as verifiers. Employers may review diploma transcripts submitted as part of a digital resume. Service providers that offer discounted fees to students can verify student ID credentials. School publishers can guarantee access to textbooks and interactive materials based on an Edulog credential, etc. In all these cases, the holders of the VCs cannot be traced by anyone through the system.

Chapter 3: Concrete User Value

3.1 Status Quo

Physical credentials are ubiquitous in our lives, but they are neither efficient nor trustworthy. Let's take the example of a university diploma as a VC to illustrate the current challenges. When a former student sends their diploma to a prospective employer, there are at least four instances of uncertainty for the latter:

1. Is the person who shows me these credentials really the person it belongs to?
2. Was the credential really issued by a trusted entity?
3. Has the credential really not been changed before the verifier sees it?
4. Is the credential really still valid or has it been withdrawn?

In today's digital economy, this lack of trust is often put up with as there simply seems to be no other option or because reducing these uncertainties would be time-consuming and expensive. In the proposed e-ID ecosystem, the issuer (accredited university), the holder (student), and the verifier (employer) would collaborate in a harmonised manner to exchange VCs. These VCs would be re-usable, instantly verifiable, secure, tamper-proof, and fully controlled by the user (i.e. student or holder).

When it comes to the actual e-ID or digital verification of 'you are who you are', we have to rely on intermediaries. The simplest example of this is arguably the credit card. By means of a bank account, a person can obtain a credit card that can be reused to some extent in the digital world to prove their identity and establish enough trust to open a customer account or purchase goods. Interestingly, a significant portion of the Internet and its transactions are based on the trust that banks are reliable and issue credit cards to people who exist physically. There are, of course, many other intermediaries and corresponding private sector solutions. These are beyond the scope of this discussion input.

The current status quo raises the question: What are the benefits that an ecosystem of digital credentials can offer to the general public, i.e. users and citizens, to the state and its various organs, as well as to the economy and its stakeholders? In the following, we address the potential benefits for each stakeholder group before outlining the shared benefits in the context of the ecosystem.

3.2. The Identity Holder (aka User or Citizen)

An e-ID ecosystem that follows SSI principles puts the identity holder at the centre and empowers them to fully own their digital identity without relying on third parties. From the perspective of the citizen and the digital consumer, this is also the biggest benefit and change from the current situation. A digital identity is no longer based on a proprietary third party, e.g. a company, and associated

credentials, but can be fully owned and managed by the holder. Take the example of social media. Today, an identity on social media is owned by the social media company, and a user gains access to it based on temporary credentials and in accordance with the company's terms and conditions. The users may not be aware of it, but the credentials they need to log in, the identity they use to move around social media, and all of their interactions belong to the social media company - if the latter decides, for whatever reason, to delete the user, the digital identity ceases to exist, regardless of the person behind the social media account (e.g. Twitter suspending Donald Trump's account).

In addition to giving the citizens power and autonomy over their digital identities, there is another important consequence - the creation of true digital identities. Instead of using identities created by third parties, we can provide identity verification during the onboarding process. This allows us to immediately identify a specific person in the digital world, without having to make educated guesses about the 'real person' behind some digital interaction or statement. In doing so, we also achieve a new level of trust in the digital space and information and interactions taking place there, knowing what can be attributed to a real person and what may be fake or based solely on unverifiable claims.

There are three types of potential benefits to this:

1. We can assume that the various onboarding processes in digital ecosystems, as well as the digital interactions taking place, do so at lower processing costs, are more convenient, and are faster. Instead of filling out forms, waiting for an SMS or the required PIN number to arrive by post, we can prove who we are, and already complete the onboarding or agree to a contract based on this verification.
2. With trusted credential verification in the digital world, the value of the digital ecosystems immediately increases for all participants, as trust in the information, interactions, and services provided is significantly higher.
3. There will likely be a significant number of new and innovative use cases and experiences that were not seen or possible before.

3.3. Government and State

For the state and its institutions, an ecosystem of digital credentials is the answer to some of the challenges that come with the current wave of digitalization. Citizens expect to have the same user experience as they do in their private digital world. However, government and other public services inherently require a higher level of trust and thus rely heavily on existing authentication and authorization processes in the real world. This dependency hinders the digitalization and digital transformation of public services and leads to the well-known cumbersome physical interactions with government agencies. It also makes these processes less efficient in parts, i.e. more time-consuming and costly.

Breaking this dependency by creating verifiable credentials will significantly boost digital services in the public sector and in e-government, reduce transaction costs, and increase the reliability of

transactions by reducing error-prone manual interactions. The cantons of Zug and Aargau are already participating in pilot projects in this regard (see Chapter 1).

An innovative ecosystem of new digital services will not emerge here immediately. But the complete digitalisation and real-time availability of existing public services for citizens, public space users, and businesses will already have a significant impact and strengthen Switzerland's position in the global economy. In addition to efficiency and economic benefits, an ecosystem of digital credentials would also favour the grassroots democracy and militia-oriented political system. Digital political election and voting processes based on an EDC could create significantly different dynamics at all levels of state, government, and society. There is the potential for such an ecosystem to embrace the digital space for political participation, discussions, opinion-forming, polling, and decision making, and to give Switzerland a further push towards a digital future.

3.4. Economy and Business Sector Ecosystems

In addition to natural persons (aka citizens, consumers, or users) and the government sector, there are numerous participants and companies of various sectoral business ecosystems that could benefit from an EDC. Not all business sectors will profit equally. As discussed in Chapter 9, use cases would start in sectors where the short- to mid-term economic benefits are obvious, resulting in a small but dedicated sectoral ecosystem of issuers, holders, and verifiers. Or, in instances where a broad stakeholder commitment can be achieved, through regulatory means or existing offerings (even if the benefits are only mid- to long-term). Two examples are given below:

The education sector could benefit by issuing digital diplomas. There is an even greater benefit if a profession is tied to regular, scheduled training and certification processes. For instance, medical doctors must attend various continuing education courses and conferences and earn a certain number of credits to maintain their licence to practice. Other professions are similarly governed, either under specific regulatory requirements or in public or military services, where a certain level of clearance or ongoing training is mandated. This could be easily established with an EDC of holders, issuers, and verifiers.

The retail sector could benefit from transparent and verified supply chains for their products. The entire digital process of buying and selling certainly benefits from the e-ID of organisations, also called Legal Entity Identifier (LEI). In theory, this could be used to better understand the various participants in the retail supply chain.

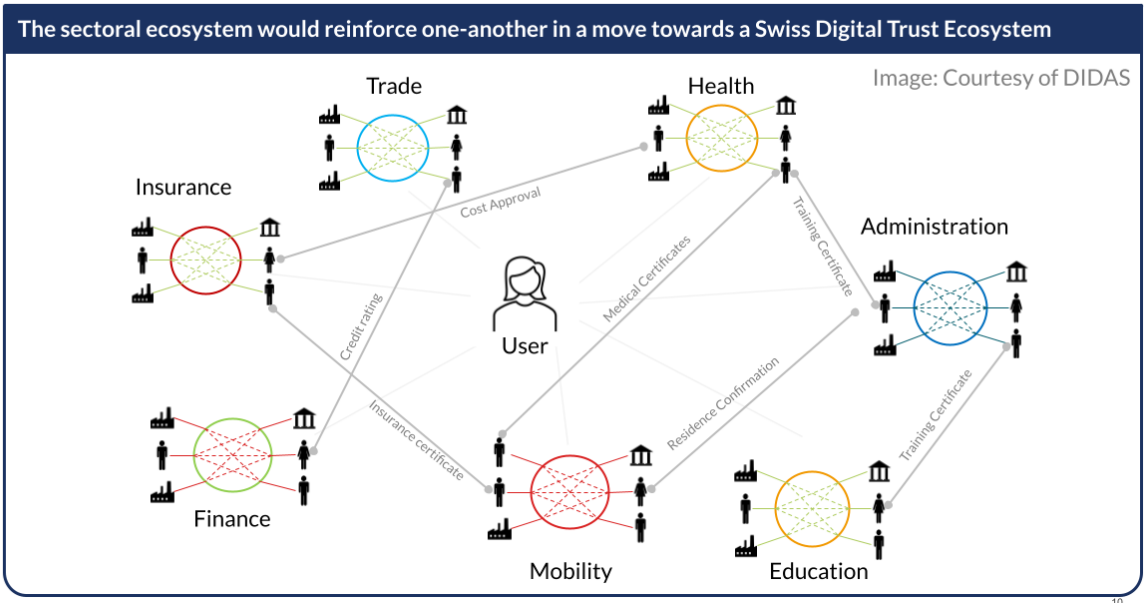
3.5. Joint Advantages, Scaling and Multiplication in Ecosystems

As already stated, there are three overarching drivers that will create value for all stakeholders. Reduced transaction costs in identification, authentication and verification will increase efficiency and

lower prices. Introducing real-world proofs in the digital space in the form of VCs will have an immediate positive impact on all digital environments and processes, as actual trust in the digital space is very limited. Lower costs and higher value will naturally increase transactions, usage, and thus the opportunity for further innovation significantly. The benefits for all stakeholders may be even greater if we look at potential combined use cases spanning all stakeholders. Indeed, these sectoral ecosystems, which are mutually reinforcing, enable a systemic shift toward a trust ecosystem.

Figure 5

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



Another dimension is the scope of the Swiss trust ecosystem. Technically, it is possible to give all entities - citizens, organisations, and even things - e-IDs and corresponding VCs. This would enable radically new use cases across sectoral boundaries. For example, the agriculture authority (one entity) could issue sustainability and organic processing certificates to farmers (another entity) who sell yogurt (another entity) to food companies (another entity). In this case, the farmer must be trusted to have produced a certain type of yogurt that meets the requirements of the organic label. Under an ecosystem of digital credentials, consumers could check the veracity of this claim and also determine whether the retailer is meeting their sustainability goals. In addition, agricultural authorities could verify the eligibility of farmers and retailers to receive certain subsidies.

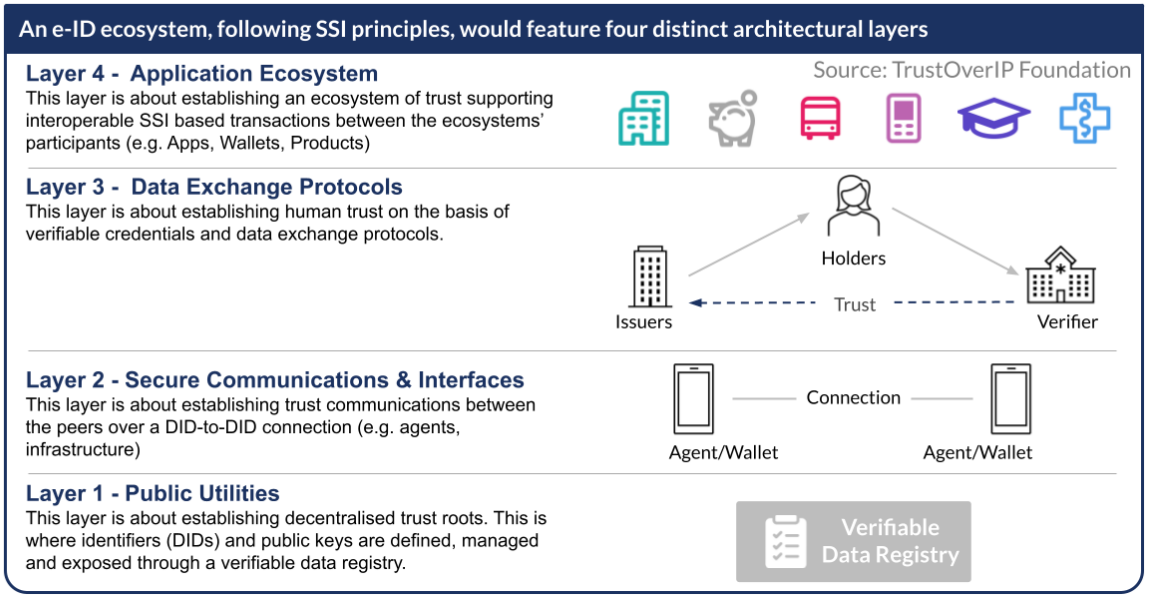
Chapter 4: Technical Perspective

This section highlights the technical aspects to be considered when implementing an ecosystem of digital credentials (EDC). We recommend implementing the EDC according to SSI principles with the appropriate technology.

4.1. SSI Components and Architectural Layers

As described in Chapter 2, SSI ecosystems consist of three roles (holder, verifiers, issuer) which communicate with each other and verify data by means of a decentralised registry. The following diagram shows the four layers, with the bottom two layers primarily focused on achieving technical trust and the top two layers focused on achieving human trust:

Figure 6



4.2. How to Create Trust?

SSI is an emerging technology. In order to use it in a trustworthy and secure manner within the EDC, we propose the following actions to be part of the governance framework:

We establish trust in the technologies and standards used: In general, the technology must have a high level of maturity. Therefore, we need robust open standards and solid reference implementations. We also need to have confidence that the implementations are of high quality. Depending on the criticality of the use cases and regulatory requirements, there must be stringent security and quality requirements for critical architectural components of an SSI solution, enforced through certification, e.g. for wallets and agents to protect user credentials throughout the credential lifecycle. For simple use cases that require less security, a lower trust level, and less stringent requirements can be applied. The Swiss government will have to define and manage the standards as

well as the certification processes to be applied to the EDC (e.g. in the form of eCH standards that complement the W3C/DIF standards and define requirements for issuers, holders, and verifiers). For specific SSI architectural components we recommend that the Swiss government publish reference implementations.

We establish trust in EDC participants: Depending on the criticality of use cases and regulatory requirements, we need to have a high level of trust in EDC participants. As part of an issuance or verification process, the holder must be able to verify the identity and rights of the counterparty (issuer or verifier). This is possible through the implementation of so-called trust anchors managed in sector-specific trust registries (e.g. swissuniversities for the universities, the Federal Office of Transport for all licensed public transport companies, or the Federal Roads Office for all cantonal road authorities). The Swiss government will need to define a solution and all processes related to the creation and management of such trust anchors. Furthermore, standards are needed for the verification of trust anchors, e.g. audit and oversight.

4.3. How to Ensure Interoperability?

Interoperability is one of the 10 guiding principles of the SSI, which states that credentials should be usable to the greatest extent possible. In the case of the EDC, interoperability at the three levels of ambition, between sector ecosystems, and from an international perspective is a critical success factor. It needs to be ensured through the use of common standards by all participants.

SSI standardisation is ongoing and several international ecosystems are evolving (e.g. IDUnion). The maturity of standards and implementations varies widely, but we expect convergence towards a set of mature standards from W3C, DIF, etc., spanning all four architectural layers of SSI. Today's major SSI platforms, stacks, and ecosystems will continue to adapt.

We recommend the Swiss government to provide direction on the selected set of SSI standards for EDC application. These standards should be aligned with the international implementation (especially the EU and the EUDI wallet initiative) and standards with priority on open source. From today's perspective, we deem it sensible for the initial implementation to be oriented towards the Trust over IP (ToIP) stack, similar to what has been done in case of IDunion and what is planned in the context of ESSIF.

Another aspect of interoperability is the interaction with existing identity and access management (IAM) solutions. SSI and current IAM implementations are complementary and can benefit from each other. For example, a VC can be used as an additional means of authentication. SSI can also leverage existing IAM infrastructure and processes. Thus, trust levels of existing digital credentials can be transferred to new verifiable credentials (e.g. using an existing x.509 certificate to issue a VC without a new onboarding process). In addition, VCs can be used for SSI-based access control (SSIBAC) in access management solutions, an important step towards a better security posture (e.g.

granting access to a user based on their business role as defined in a VC). This interoperability with existing IAM solutions can be enabled by so-called bridge solutions (e.g. OIDC bridge) permitting to leverage existing identification standards such as OpenID Connect.

4.4. How to Implement?

There is no better way to understand a new technology, assess its potential added value and limitations, and foster innovation than a real-life implementation based on representative use cases. In the case of EDC, we recommend an agile implementation of a sandbox across the four layers with proofs of concept (PoCs) and pilots to validate the standards and establish a reference implementation. With this approach, also proposed by the Digital Identity and Data Sovereignty Association (DIDAS), we could lay the foundation for the productive use of the technology and governance framework and generate value. Ideally, the selected use cases should be cascaded across sectoral ecosystems (e.g. using university diplomas within an application process). In addition, these implementations could be accompanied by a crowd security initiative such as a bug bounty program.

Chapter 5: Governance Perspective

The main role of the EDC governance is to guarantee an appropriate level of trust in all transactions it facilitates or supports. A substantial challenge arises with *ambition level 3* as it increases the number and diversity of actors with respect to levels 1 or 2. While an initial approach with ambition level 1 or 2 would be somewhat easier to implement and govern, we propose starting directly with ambition level 3 for the following reasons:

- To maximise the benefits of a government-issued and guaranteed e-ID, it must be able to support as many everyday use cases as possible with high user-friendliness. Only ambition level 3 removes the barriers between public and private sector use cases.
- The lack of support for private sector use cases in the e-ID ecosystem would motivate the creation of separate structures to accommodate such use cases. This has a number of drawbacks:
    - It would fail to produce the intended learning outcomes needed or a future integration into a single e-ID ecosystem.
    - The cost and effort to set up the ambition level 1 or 2 infrastructure would have to be borne entirely by the public sector.
    - Since pure public sector use cases are rare for most residents, large-scale demand for the e-ID will be difficult to achieve and support will become comparatively expensive (see also Chapter 6).
    - The industry will be pushed to build parallel infrastructures outside the regulatory framework of the e-ID ecosystem and possibly use an incompatible technology base. This would make later integration even more difficult.

SSI is able to combine credentials from different sources, which is a key feature for supporting the large number of contributors expected in an ambition level 3 ecosystem. It is the responsibility of the governance framework to ensure a sufficient level of trust in the information provided in this way. How can this seemingly daunting task be accomplished?

5.1. Human Trust

We see value in establishing new governance structures specifically tailored to the EDC only where strictly necessary, and would otherwise advise relying on existing structures in the analogue world and linking them to the EDC. We would therefore enable existing actors and structures to carry their current analogue-world role into the new SSI world of the EDC. In this way, we could achieve an alignment of the governance of existing ecosystems with the EDC's governance:

- It is sensible that existing authoritative sources of a given type of information would act as issuers of VCs within the e-ID ecosystem. This is best illustrated by an example: The Rectors'

Conference of Swiss Universities (swissuniversities) maintains a list of recognised or accredited higher education institutions in Switzerland which constitutes an important source of information for validating university diplomas. swissuniversities could make the accreditation status of universities available as a verifiable credential to the verifiers who check the validity of issued diplomas. Similarly, the commercial register could become an issuer of VCs on the basis of the information contained in its register.

- An important trust anchor in the analogue world for identifying individuals is the government-issued personal ID card. The e-ID will play the same role in identifying people in the digital world. To leverage the existing human trust in the ID card, we propose that the e-ID be aligned as closely as possible to the lifecycle processes of the ID card and issued by the same body.

5.2. Verifiable Data Registry

The registry is a publicly readable repository of the cryptographic evidence necessary to validate verifiable credentials. It acts as a trusted source of information for all stakeholders in the e-ID ecosystem. In particular, it assists verifiers in validating proof, e.g. assessing whether required certifications or accreditations are available and have been issued by authorised parties. It is worth noting that the registry does not store verifiable credentials and thus does not contain any personal information.

Given international comparisons, the following principles seem sensible around the verifiable data registry.

- A governance structure where the federal government has overall responsibility but can delegate as much as possible to appropriate bodies.
- A permissioned, public ledger based on blockchain technology under the direction of the federal government as the foundation of the Swiss e-ID ecosystem.
- An emphasis on its decentralised nature and increased trust and resilience via the sharing of selected operational tasks of the registry with private parties where appropriate (see also Chapter 4).
- A governance framework that follows international best practices use cases for public sector and private sector

5.3. Trust Registries / Sector Regulations

The sectors that are to participate in the e-ID ecosystem can be considered as *sector-EDC*, able to define their own standards and procedures in many areas. These sectors could successfully operate their own human trust anchors by promoting labels and brands, and they could also operate a sector-EDC on their own - unless the EDC is attractive enough to be used for sector purposes as well. The more sectors that participate in the EDC, the more they can all profit from cross-sector use cases,

such as reusing VCs from other sectors and offering their own to others.

The following principles and recommendations seem sensible to make the EDC attractive to other sectors and thus transform our EDC into a true *ambition level 3 EDC* that benefits from the advantages outlined at the beginning of Chapter 5:

- The government acts as the governing body for the EDC as a whole, providing appropriate technical trust anchors (e.g. in the verifiable trust registry) and human trust anchors (e.g. regulations and processes). The EDC framework should allow for the inclusion of sectoral trust anchors (e.g. through accreditation or auditing) with reasonably lightweight procedures.
- All sectors are affected in many ways by the regulatory frameworks of public authorities. These frameworks should be reviewed to best support (or at least not hinder) EDC adoption.
- The government might consider creating human trust anchors for trusted verifiers by providing accreditation processes and promoting trust labels. Wallets might use this information to help holders decide which attribute to present to a verifier before submitting potentially sensitive information.

5.4. e-ID (eGov sector) and Wallet

While the e-ID is technically only one verifiable credential among many, we expect it to act as the trusted *identity basis* and thus become the credential most commonly used in cross-sector use cases.

We anticipate that the e-ID requirements will have a significant impact on other components of the EDC and will define the boundaries for the e-ID ecosystem in general.

- Alignment with e-ID approaches in other nations and regions, in particular the EU, should be pursued to facilitate support for future cross-border use cases.
- In case the government creates its own wallet, we hope that there will not be any regulation to hinder the development of a complementary “market of wallets”. For this, the government would have to formulate clear criteria for wallets.

Chapter 6: Legal Perspective

6.1. Legal Classification

Secure identities form the basis for legal proof and are thus an indispensable prerequisite for business and societal relationships. In the physical world, the government issues conventional means of identification for this purpose, namely, in the case of Switzerland, the Swiss passport, the identity card, or the alien identity card. In addition, it should now also be possible to prove the identity of a natural person electronically. State-recognized e-IDs will enable holders to identify and authenticate themselves in digital space as well. Wherever no specific regulations or requirements of the involved parties apply, and a business transaction can be completed with immediate payment, no further proof is usually required to complete a transaction.

In this field of tension, concepts such as the self-sovereign identity (SSI) approach aim to fulfil data protection concerns such as the principle of data minimization as best as possible through self-managed identities and attributes. At the same time, the other requirements of the actors involved, especially user-friendliness (see Chapter 9), are to be considered by conceptually linking them to familiar processes from the physical world. Such a trust ecosystem ultimately forms the basic infrastructure for a digital landscape, on which existing applications can become widely established and new applications can flourish. Much-discussed examples of this are the electronic patient dossier, e-collecting, and e-voting systems, the ordering of register extracts of all kinds, and, of overriding importance, the digital declaration of will by means of electronic signatures. Widely available, recognized electronic identification means therefore form an elementary building block in a more comprehensive e-ID ecosystem that can establish security and trust in the economy. As a result, sophisticated business transactions with the state as well as between private individuals can be conducted electronically and thus more efficiently as well as independent of location and time.

In addition, they form a basis for trust services, such as the electronic signature, which are offered in Switzerland and the EU by private trust service providers in accordance with strict regulatory requirements, but are not part of the e-ID.

6.2 Constitutional Dimension

It is a general achievement of the democratic constitutional system that laws grant us legal rights and that there are courts to ensure their enforcement. The COVID-19 pandemic has shown how important it is to significantly improve digital access to these courts, but also to the authorities in general.

According to the Federal statistical office (FSO) survey on Internet use in Swiss households, the proportion of Internet users among the adult population of Switzerland continued to increase. From 84% in 2014, it rose to 90% in 2017 and 93% in 2019. Accordingly, by age, almost all people between

15 and 55 use the Internet, 95% of them daily. The biggest increase is seen in the highest age groups. 88% of 65-74-year olds used the Internet in 2019 (up 11 percentage points from 2017). The numbers for Internet use in a professional context are even more impressive: 87% of employed people in Switzerland use a computer or other electronic equipment at work. 57% work with specialist software and nearly 40% are given their tasks or instructions via a dedicated application.

Today, media disruptions (germ. Medienbrüche) occur wherever formal requirements block the digital path and there is no access to a legally compliant digital alternative, or when evidence is only physically available. A national infrastructure enabling the state and private parties to issue and verify digital evidence is therefore a necessary component for exploiting the value creation potential of digitalisation and maintaining the high level of legal certainty relevant to Switzerland as a location in the medium and long term. Finally, it should be noted that (identity) proof is regularly required, especially for use cases of high importance such as official business or judicial proceedings. In view of the high level of use of the Internet across all population groups, the current lack of a digital trust infrastructure also de facto impedes access to essential public services.

In summary, creating a reliable digital trust ecosystem fills an essential gap, as the lack of trust elements in digital transactions is the biggest barrier to digitalisation today. Addressing this shortcoming will create a solid breeding ground for the future digital economy and high-quality e-government services.

6.3 Requirements for the Legal Framework

A concrete proposal for the regulation of an SSI-based e-ID approach is still pending. Nevertheless, the following core elements for the legal framework can be derived from the lessons learned from previous attempts to establish a national e-ID solution and from similar foreign projects:

- A Swiss e-ID solution in line with international e-ID solutions, in particular with the solutions in the EU, would be preferable (no “Swiss finish”).
- The federal government should be primarily responsible for the legal framework of the decentralised network. However, the possibility of jointly operating this network with other actors should not be ruled out.
- The legal framework should set the guardrails for innovative private sector offerings in the area of digital trust.
- We anticipate a wallet-level market (i.e. a multi-wallet market), in parallel with a wallet by the Federal Government (should this be provided).
- In addition, the creation of a comprehensive e-ID solution will have far-reaching implications for existing legislation, which need to be considered in terms of the entire ecosystem.

First and foremost, the Federal Act on Identity Cards for Swiss Citizens (SR 143.1) seems to be affected by the matter. ID cards under this law serve to prove the holder's Swiss nationality and his or her own identity. However, it is generally understood that the legal scope of an e-ID is less far-reaching. It neither confers citizenship rights nor does it serve as proof of Swiss citizenship, for example when crossing national borders. Rather, it is intended to serve its holder merely for online identification and authentication.

This should also enable financial institutions and casinos subject to the Anti-money laundering act (AMLA) to carry out secure electronic identification. e-ID credentials should therefore be considered as evidential documents within the meaning of Art. 3 of the Anti-money laundering act of 10 October 1997 (SR 955.0). The Anti-money laundering act itself does not conclusively regulate what constitutes an evidential document but leaves it to FINMA's money laundering ordinance to define this in more detail. If necessary, this ordinance should be adapted so that e-ID credentials can be used in electronic business transactions with financial institutions and casinos. Furthermore, the Federal act on certification services in the field of electronic signatures and other digital certificate applications (RS 943.03) as well as all relevant FINMA circulars on personal identification should also be adapted to include this new method of electronic identification.

Finally, extending the view to the ecosystem of digital credentials, it must be ensured that further use cases such as age verification when purchasing tobacco products or alcoholic beverages or check-ins in the tourism sector are legally harmonised across sectors (e.g. standard use cases). Standardised requirements should even be considered in these areas to the extent necessary. This is the only way to ascertain that market participants in the ecosystem can operate such solutions economically and sustainably. User-friendliness also means that a hotel check-in in Geneva, for example, is no different from a hotel check-in in Adelboden. Precisely because these are purely technical requirements, a federal legal framework for this appears to be a sensible solution.

Chapter 7: Usability Perspective

7.1. Focus on User-Friendliness

Usability is one of the most important aspects and crucial for acceptance and adoption of the Swiss e-ID ecosystem, as it complements and partially competes against the long-established physical identity card or other physical credentials. For most users, the digital wallet is the part of the e-ID ecosystem they interact with most often and thus embodies the EDC in their eyes. This must be given the utmost attention. Other areas where usability plays a major role include the issuance, verification or withdrawal of VCs, all of which are important process steps.

7.2. Requirements for a Digital Identity Wallet

It is important to note that even the physical ID card has weaknesses and does not provide 100% protection against counterfeiting. Also, not all security features are checked at every point. These aspects have to be considered when discussing the potential security gaps of any new solution. Below is a preliminary list of key requirements that could be relevant for a digital identity wallet.

- The wallet solution must support all popular mobile devices.
- VCs must be usable on different devices.
- Two-factor authentication should be used whenever possible as a security feature, as should biometric information. It is worth noting that there are different levels of security and that not every identity requires maximum protection, just as in today's physical world.
- In the context of physical interaction, the wallet must also function offline or in situations without Internet connection.
- To create and restore a backup must be as automatic and effortless as possible.
- The rollout of software updates must be as smooth as feasible. At the same time, it must be factored in that many users do not or only irregularly update their devices. This should affect the use of the wallet as little as possible.
- Setup and operation should require a minimum of steps and be easy, even for inexperienced users.
- There must be maximum protection against phishing or other attempts to steal VCs. This is particularly important in situations where a VC must be shown or passed on quickly and unreflectively.
- The unknowing or knowing disclosure of a VC must be made as difficult as possible. This means that the verification of a credential must establish that the wallet belongs to the specified user (e.g. through photographic proof).
- Just as with physical documents, such as ID cards, passports, etc., and unlike with centralised digital accounts, the introduction of VCs under SSI principles implies that the responsibility for managing these credentials is transferred. Holders are responsible for storing and managing their VCs. This transfer of responsibility has the added benefit of

ensuring that there is no single point of attack. This needs to be backed up by awareness campaigns.

Of course, this list is by no means exhaustive. The development of a digital wallet calls for a detailed list of functional and non-functional requirements.

7.3. Issuing and Verification Process Requirements

As outlined earlier, the wallet is the central user interface for the e-ID and other VCs. For most users, it is the primary point of interaction with respect to their identity. Nevertheless, the processes around issuance and verification are also critical.

For these processes, the following requirements exist:

- Issuing and revoking a VC must be simple, fast, and straightforward. It should preferably be done digitally so that no physical presence is required.
- According to current research, our society is struggling to adopt yet more new technologies. It is therefore important to introduce the EDC by implementing processes that are as similar as possible to those used with other technologies. In fact, they should even simplify these processes since the EDC will reduce the number and variety of already existing verification processes.
- Verification of a credential needs to be as simple as possible and without interface issues. QR codes are a very good option for interaction between the wallet and a business application; the COVID certificate is a case in point.
- The processes for generic use cases (e.g. sign-in) need to be as consistent as possible across all participants, creating a certain standardisation and thus a logical flow for users.
- The fact that verifiable credentials are managed for other individuals, e.g. for children or persons lacking legal capacity, must be taken into account.
- New features such as the zero-knowledge proof must be designed to be understandable and comprehensible. The technological background does not need to be understood, but the benefits and features should be communicated to all users by means of examples.
- The introduction of the digital identity wallet should be facilitated with the help of factsheets, videos, support, and training. This is critical to achieving broad acceptance. It is important to remember that all of us were introduced to the use of physical solutions as children. For future generations, the same will be true with respect to the new digital solutions.
- By involving experts in usability research and considering the lessons learned from current digital identity solutions, it is possible to develop an identity solution that is

easy to use and user-friendly. Today's physical solution also has its weaknesses and flaws and, most importantly, is not designed for a digital future.

The e-ID is an important complement to the existing ID card or passport and is primarily designed for interaction in the digital world. In the future, it will most likely be the primary means of proving one's identity. As explained above, other VCs and their combination with the e-ID are crucial in our digital lives. For some people, they will be more important than for others. For some use cases, a verifiable full identity of a person will be necessary, for others only single credentials will suffice. This diversity in society has to be acknowledged when discussing and adopting digital identity and digital credentials. In this regard, a comprehensive strategy on digital inclusion would be sensible.

Chapter 8: Economic Perspective

In many situations, the biggest obstacle to digital transformation is the lack of customer trust. This can take different forms. First and foremost, it can be due to users fearing the potential risks of a new technology and therefore shying away from adopting it. Second, it may stem from the tendency to strongly underestimate the long-term benefits based on the experience that the promised potential of new technology is rarely fulfilled in today's society. As a result, in the public's perception, both the short-term costs and risks outweigh the benefits, compelling them not to use the technology. Third, it can be an excuse to reject a change of professional practice brought about by a technological solution. For example, in countries that have implemented the inter-organizational sharing of patient data through electronic patient files, many medical doctors claim reluctance to share data for fear of misuse. In reality, they are far more concerned about insurance companies using the data to control their therapeutic decisions. Fourth, the lack of trust may take the form of endless political discussions in the media or in parliament. The debate over the use of social security numbers to identify citizens is a typical Swiss example.

Regardless of whether there is actual distrust of technology, resistance for other reasons or lack of clarity as to citizens' actual thoughts about a solution, the discussion of the trust problem significantly delays the necessary measures to ensure technology deployment. For example, deficits in user experience are usually hidden behind security and trust discussions, as in the case of the Austrian Electronic Health Record ELGA as the main e-Health backbone. Solving the trust problem is therefore the biggest challenge in many sectors, blocking digital transformation in numerous cases for more than a decade. The opportunity costs of the unsolved trust problem are likely very high, although it is not possible to adequately quantify them.

Unfortunately, the trust problem is a complex social problem. In the past, we have seen many failed attempts to solve complex social problems with simple technological solutions. The principle of requisite complexity tells us that this is to be expected. Social problems require technological solutions that reflect the complexity of the original problem. These solutions should preferably be based on established cultural practices without copying analogue processes. In other words, they should exploit the new degrees of freedom in the design of digital solutions without requiring any kind of new thinking from the users. This is especially true for the trust problem depicted above. In essence, the technological solution should complement and simplify existing trust practices rather than invent new ones.

8.1. Value for Switzerland

The e-ID ecosystem of VCs provides a solution to the digital transformation’s trust problem that adequately addresses the requisite complexity. It establishes a distributed trust anchor for the digital transformation of the economy in Switzerland. In doing so, it creates a trust space based on culturally

valid trust principles and practices and extends them to the digital world. The resulting trust space is anchored in a democratically controlled government, but fully owned by citizens. Thus, it combines self-sovereignty with good government. In particular, the e-ID ecosystem does not require citizens to adapt their fundamental judgements since it is rooted in analogue trust. Citizens only have to learn how to handle the digital tools, but do not need to acquire new world models. This makes it more likely that widespread adoption will eventually occur. The fact that no one other than the citizens decides how their credentials are used will keep distrust in the ecosystem to a minimum. The overall design also reduces the risks of actual systemic misuse of personal data. Thus, trust is underpinned by the technological trustworthiness of the entire ecosystem. In this way, the e-ID ecosystem helps accelerate the digital transformation of the Swiss economy and society, which in turn increases the competitiveness of the Swiss economy as well as the social and economic attractiveness of the location.

The ecosystem of digital credentials also contributes to digital sovereignty in Switzerland. At the individual level, citizens can control the use of their VCs, at the organisational level, companies and institutions control the issuance of VCs, while at the national level, Switzerland as a country has full control over the trust anchor. Due to interoperability properties, the e-ID ecosystem will be compliant with the emerging ecosystems in other countries as well as with the European ecosystem around the digital wallet that will replace the eIDAS concept and infrastructure. In this way, Swiss citizens and companies would not have to adapt to foreign solutions for activities across Europe. Likewise, foreign nationals would be able to use their credentials in Switzerland without adaptation.

So far, however, there are still some limitations. The EU Commission's current requirements under the proposed new eIDAS regulation stipulate that the wallet must be implemented with the EU toolbox, failing which it is not possible to be part of the trust registry or bring the EU VCs into your wallet. Nonetheless, the basic interoperability in terms of all dimensions of the European interoperability framework (EIF) provides a good foundation for the future unlimited and unhindered cross-border use of digital credentials.

To summarise: The ecosystem of digital credentials, by design, creates a sustainable solution to the trust problem. It thus reduces the obstacles on the path to the digital transformation of the Swiss economy, helping it to grow. In addition, it strengthens digital sovereignty and thus creates public value for Swiss society.

8.2. The Complexity Challenge

The e-ID ecosystem provides small, ever-growing benefits to many actors, but also imposes costs on them. Strong network and economy of scale effects occur. The more actors participate, the greater the benefits for all participants. The costs of having more actors in the system are zero for a single actor, and the marginal costs of issuing and holding more credentials or presenting and verifying them

more often are very low. Consequently, the potential benefits to individual actors depend on the size of the ecosystem, i.e. the number of credential holders, credential issuers, and verifiers, while the individual costs are independent of the size of the ecosystem.

More issuers and more verifiers implies that credential holders can use credentials in more situations, while their costs stay nearly the same. The time costs for installing a digital wallet (and the financial costs that may be incurred) are much higher than the costs for using it, i.e. for presenting credentials to verifiers. Thus, the overall costs will be offset only if there are enough usage opportunities.

More credential holders and more credential issuers implies that verifiers can benefit more often from established verification processes, while their costs remain essentially the same. The cost of setting up these procedures and the necessary infrastructure is much higher than the cost of conducting verifications. Thus, the overall costs are compensated only if enough people use these procedures.

Finally, more credential holders and more credential verifiers means that the issuance of paper certificates can be replaced in most cases on the credential issuer side, with costs again remaining essentially the same. The cost for setting up the issuance infrastructure and the issuance processes is much higher than the cost of issuing a verifiable certificate. Thus, the overall cost will be only offset if enough paper documents can be replaced with digital credentials.

In other words, when building the e-ID ecosystem, we are dealing with a version of the *chicken-and-egg problem* involving three groups of actors (instead of the two groups of actors in the classical chicken-and-egg conundrum). The ‘first copy costs’, i.e. the costs for putting in place the necessary infrastructure and processes, and the costs for running the infrastructure are many times higher than the costs of operating the processes in an actual use case. The decisive factor for a successful solution to the chicken-and-egg problem is therefore the number of uses. As long as this number is low, there is little incentive for stakeholders to participate in the ecosystem.

It is important to note that the presented chicken-and-egg problem is not a purely quantitative one. It also involves a qualitative aspect, namely diversity. The ecosystem as a whole benefits from both a few highly attractive single-use cases and a wide diversity of the many other verification use cases.

8.3. How to Solve the Chicken-and-Egg Problem

There are many experiences with the chicken-and-egg problem in the technological context, some of which are rather unfortunate. Usually, full adoption does not occur immediately, but with longer delays. In general, technological progress and the economic use of the technology do not run in parallel, which may in fact prevent the rise of a new technology. The only way to overcome these problems is to make sure that: a) there is a wide range of usage options with tangible added value, and b) people are aware and committed pioneers are exploring enough of these options.

In general, there are six principles that we can learn from to build the Swiss Trust Ecosystem:

1. The larger the optional system, the more likely it is to be adopted. Consequently, a level 3 ecosystem has a much greater chance of becoming successful than a level 1 or level 2 ecosystem.
2. The low cost of use is a necessary condition for solving the chicken-and-egg problem. Therefore, as an infrastructure component of the e-ID ecosystem, the verifiable data registry should be provided by the government as a public service.
3. Communication must take the difficult route of explaining the underlying concept, rather than telling simplistic stories that reduce the big picture to trivial or even atypical use cases.
4. Pioneering efforts must be supported in effective ways. Relying on the lucky emergence of enough pioneers without supporting this process carries a significant risk of delay or even failure. Instead, a strategy is needed as to which activities and fields of action should be prioritised.
5. Building an ecosystem cannot be fully planned in advance, nor can it be fully carried out ad hoc. Instead, it is necessary to implement a clear strategy in an agile manner and adjust plans according to observed successes and failures.
6. Examples from abroad show that if the use of verifiable credentials from the e-ID ecosystem is made mandatory for accessing e-government services, adoption significantly increases. In contrast, failure to adopt key e-government services undermines trust in the e-ID ecosystem.

Chapter 9: A Possible Roadmap

In December 2021, the Federal Council called for an e-ID ecosystem based on a state-operated infrastructure in its directional decision. We outline a possible roadmap of what an e-ID ecosystem could look like in the Swiss context. This is of course based on preliminary information and is thus largely hypothetical. It is merely a first attempt to understand what is to come. It is by no means comprehensive and is intended to be iterated upon as new information becomes available.

9.1. e-ID, e-ID-backed Digital Signatures, and Digital Driver's Licences

The starting point for the formation of the e-ID ecosystem will be the issuance of the e-ID itself, together with e-ID backed digital signatures. The Swiss government has the political mandate for this implementation. It must be stated again that in an EDC, the e-ID, while being the most important VC, remains one VC among many. In other words, the e-ID as a means to enable citizens to authenticate themselves in a trustworthy manner is a core element of the EDC. It is our understanding that the e-ID credentials can be used universally for trusted identification and for the application of digital signatures. The issuance of the e-ID and subsequent e-ID-backed digital signatures will therefore be decisive milestones in the development of the EDC in Switzerland. This will actually set in motion two parallel efforts. One includes initiatives driven by the federal government, while the other entails initiatives driven by the private sector and academia. We will discuss both in turn.

In addition, VCs for driver's licences, which are being developed in a pilot project by asa and FEDRO (see Chapter 1), may become a core part of the EDC. Legal foundations already exist in this area. Moreover, it is already planned to extend this pilot project to navigation licences.

9.2. Subsequent Government Efforts

The issuance of the e-ID and subsequent e-ID-backed digital signatures opens up two options for the government:

1. **Use of government-issued VCs and the e-ID for e-government processes**
   Citizens' adoption of e-ID would be greatly enhanced if all e-government services requiring authentication accepted (or even required) the use of an e-ID. This, in turn, could be pushed by providing open-source components that can be used by government agencies on all federal levels to implement the authentication process via e-ID. Similar support through open source components has already been successfully implemented abroad, e.g. at the national level in Austria for the 'Handy-Signatur' and at the supranational level in the EU for the eIDAS nodes (see Chapter 1).

2. **Use of externally issued VCs for e-government services**
   Many mandatory e-government processes require relevant declarations from third parties. Tax

declarations, for example, typically involve declarations of income, accounts balances, and expenses. Theoretically, these tax-relevant statements could be issued as VCs by the relevant organisations. Since they have to issue the declaration anyway, they do not need to set up new processes, but simply add the possibility of VC issuance to existing processes that can be automated. This would eliminate media disruptions, with some benefits for users and significant benefits for the government agencies involved. One way to move this forward could be to require organisations to provide VCs on demand in selected cases. Some of these VCs could then be reused in business transactions.

In this context, it is important to note that the federal government has announced two EDC projects. One is a pilot project for digital driver's licences, for which a legal basis already exists. The other is a proof-of-concept (PoC) project for digital VCs intended for federal employees (see Chapter 1).

9.3. Subsequent Ecosystem Efforts

The issuance of e-ID and e-ID-enabled digital signatures will provide opportunities for the ecosystem, notably the private sector and academia, to initiate use case scenarios. In light of the chicken-and-egg problem (Chapter 8), it will be important to prioritise the fields of activity. Two types of usage scenarios are most likely to succeed. The first involves instances where the short- to mid-term economic benefits are evident, resulting in a small but committed sectoral ecosystem of issuers, holders, and verifiers. The ongoing SSI efforts fall into this category (see Chapter 1). The second are cases where a broad stakeholder engagement can be achieved through regulatory means or through existing offerings (even if the benefits are mid- to long-term only). For instance, these could include efforts around membership cards. The two following sectoral scenarios are built on this basis:

1. **Academic Institutions Issuing VCs to Students**
   Universities can issue all kinds of diplomas (as well as of course student IDs) as VCs. They can also require VCs for enrolment in courses or matriculation. Investing in this sectoral ecosystem is a means for universities to become digital transformation pioneers. Lagging behind is not an option for individual institutions, as it might affect their position in an increasingly competitive market. The economic benefit of this usage scenario is the simplification of document verification, which will allow a lot of time to be saved and increase the flexibility to set up courses on an ad hoc basis. In the long run, academic certificates as VCs will help streamline the accreditation process and reduce the possibility of fake diplomas while improving organisations' recruitment efforts. This is a case in point where the short- to mid-term economic benefits are obvious. As a result, a small but engaged sectoral ecosystem of issuers, holders, and verifiers may emerge.

2. **Organisations Issuing Membership or Affiliation Status to Employees**
   Companies, institutions, and associations can issue VCs of membership or affiliation status to their employees, partners, or customers. These VCs can then be used to gain access to digital or

analogue resources (e.g. access to buildings). In most cases, organisations need to issue some form of credentials anyway. Thus, they just have to extend existing processes for allowing the issuance of VCs. VCs help them to automate access control digitally and save money on membership cards, while VC holders no longer need to carry around large stacks of analogue membership cards. As a side benefit, organisations can standardise their access control systems, which simplifies related procedures, saves time, and improves security.

3. **Other Promising Use Cases**

   There are further promising use cases that merit closer investigation. These include verifiable credentials in healthcare, e.g. to reliably document the education and training of professionals or the insurance status of patients. Furthermore, VCs for account status could be offered as a service in banking, depending on the market sector and the business strategy, or companies could issue VCs to their legal representatives. Once the ecosystem is established through the efforts outlined before (Chapter 9, as well as points 1 and 2 in this Section), there is an opportunity for companies and other organisations to promote use cases as innovation, either by adopting verification practices and acting as verifiers or by issuing new types of verifiable credentials.

9.4. Use Case Development

The question remains how to concretely address the above usage scenarios. Innovators will have to deal with the following issues:

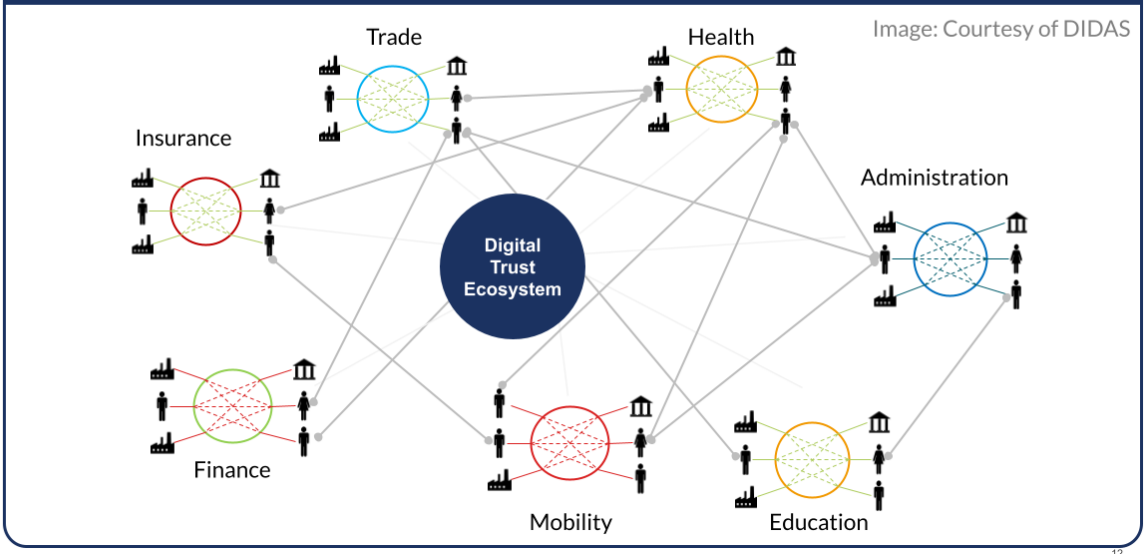
1. How to move forward when expectations are high while many unanswered questions seem to halt progress?
2. How can we demonstrate the value of an ever-evolving technology before all open questions have been clarified?

In light of this contradiction, we propose a two-stream approach to implementing these usage scenarios. The main goal of *stream 1* is to show, not to tell. In a sandbox-like test environment, practical use cases of all types and for all sectors could be developed and demonstrated to people who are not yet familiar with the concepts associated with an e-ID-Ecosystem. Initial sandbox-like environments already exist in the Swiss market. In such environments, prototypes or minimal viable products (MVPs) could be built based on frameworks readily available for the underlying decentralised trust network. These applications will never go directly into production, but serve to demonstrate the interaction of all players in such an ecosystem. The proposed federal law on the use of electronic means to fulfil government tasks (EMBaG) supports stream 1 projects. Its final form will define the specific setting for these projects. However, stream 1 projects could also be implemented in the private sector.

The goal of *stream 2* is to design and build the infrastructure, tools and governance required to create a solid, secure, and internationally interoperable foundation for a Swiss e-ID ecosystem, including the digital wallet. Here, the federal government is predestined to play a leading role. Ideally, these two streams will run in parallel and cross-fertilize each other. This presumes that there are communication channels between the two streams to exchange experiences and perspectives.

Figure 7

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



We believe active interaction between academia, industry, government, and the general public is essential for the successful deployment of an e-ID ecosystem in Switzerland. An orientation towards the quadruple innovation helix concept would be particularly expedient here. Only in the spirit of collaboration, transparency, and inclusion can we move towards a Swiss trust ecosystem that will deliver on its promises.

Chapter 10: Open Questions

1. *What happens when a digital wallet is lost? How does the backup work?*
2. *How would digital signatures work as part of the e-ID?*
3. *What exactly does the management of the trust registries look like?*
4. *How exactly will verifiers be approved to participate in the trust registries?*
5. *Will the federal government also issue its own wallet? If so, will it be mandatory? What kind of private sector involvement can be expected? And if not, will the federal government support wallet solutions in other ways (e.g. through standards or developer kits)?*
6. *What is the practical interplay between trust anchor and user control?*
7. *How will international technology and electronics companies react to digital credentials from a government-controlled ecosystem?*