Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Federal Office of Justice FOJ

Discussion paper on the target vision for an e-ID

Basis for discussion for a common vision of a governmental electronic identity with a view to the Federal Council's upcoming policy decision

Summary

This target vision for an e-ID serves as a basis for public debate. It does not aim to decide on an option for a new, governmental electronic identity (e-ID). The focus of the public debate is on the possible benefits and use cases of an e-ID and the demands on a governmental e-ID. The outcome of this public discussion will then serve as the basis for a policy decision by the Federal Council to be taken by the end of 2021.

For Switzerland, the search for an e-ID solution begins anew. As a first step, the vision for a new e-ID is to be discussed. The focus is on the following questions:

- Is the e-ID a digital identity card issued by the state to prove one's identity, and can it be used in the analogue world as well as the digital world?
- Could a greater ecosystem with digital proofs of all kinds from a wide variety of public and private providers give rise to a greater benefit and accordingly also broader use by holders? What would the risks be?

The emphasis of the discussion must be on the benefit of an e-ID for its holders. A few example use cases are outlined, in the knowledge that there is no *one single* use case, but rather that the sum of the benefit of all use cases will make the e-ID a success. At the same time, however, it must be recognised that the need of a wide range of public and private service providers for an easily integrable, openly designed e-ID ecosystem is currently presumably greater in the short term than that of the actual holders of an e-ID. Accordingly, it is crucial that suitable use cases are able to show the concrete benefit for holders as well. In this context, the state has the additional roles of initiator, enabler, and guarantor.

The background for this discussion has changed since the original e-ID Act was rejected in a national referendum, including with respect to the following areas:

- Data protection and, in particular, the protection of privacy have become an even more important topic in public discourse.
- Future identity systems will be based on user-centred approaches.

In terms of technological implementation options, several approaches to solutions will be laid out as a basis for discussion:

- Self-sovereign identity
- Public key infrastructure
- Central governmental identity provider

All approaches give rise to open questions; not every approach covers all requirements equally well. Evaluation of the approaches is not covered by this target vision for an e-ID, however. This must occur as part of a public debate in which the main outlines of a common vision for an e-ID, its use, and the demands on the ecosystem emerge. Public debate will contribute significantly to the Federal Council's policy decision planned for the end of 2021. Following this policy decision, the legal basis can be developed, which must then be decided by Parliament.

Glossary

Attribute	Single data point, e.g. given name or date of birth
Credentials	Term in the SSI context: Dataset consisting of one or more attributes Term in the IdP context: Login credentials: Characteristics of identity that enable authentication of the subject, synonym for authentication factors, e.g. username, password or PIN
Data minimisation	Two aspects are subsumed under the term data minimisation: Reduction to the minimum necessary attributes when transmitting data to third parties, and avoidance of unnecessary data flows and the associated marginal data.
Decentralised data storage	Data is not kept in a single, central storage but rather is distributed across a network of storage systems or is offloaded to end-user devices.
Decentralised identity	Electronic identity that is not managed by a central system and can be used only by way of that system, but rather is stored on the user's smartphone, for example, and can be used directly through such a device.
Digital trust infrastructure	A set of regulations, processes, concepts, and infrastructure elements that ensure trust in digital processes and their process fidelity and are accepted and used by a broad public.
e-ID	e-ID stands for governmental electronic identity – a kind of digital proof that users can employ to prove their own identity.
e-ID ecosystem	Interaction of a wide variety of actors (public and private) with different uses and offerings, taking place with and around the e-ID and on the basis of a jointly used digital trust infrastructure.
eIDAS Regulation	eIDAS stands for "electronic Identification, Authentication and trust Services" and is an EU regulation defining uniform rules governing electronic identification and electronic trust services.
Holder	In the context of SSI and PKI, the holder stands for the owner of a wallet containing digital proofs.
Identity hub backup	Electronic backup facility of identity proofs 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	Identity and access management are often referred to together under the abbreviation IAM. Identity management is responsible for the management of identities and the assignment of properties (technical attributes) – independently of the associated roles and privileges. In this context, an identity can also be understood in simplified terms as a login or account.
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 verified credentials.
Issuer	Institutions, organisations, and also private individuals who issue a digital proof and hand it over to the user.
Level of ambition	Term from the revision of the eIDAS Regulation (level of ambition) to clarify the scope of the use of an e-ID infrastructure.
Node	Storage node in a distributed storage network (distributed ledger, DLT)
Peer-to-peer communication	Direct communication without an intermediary. In the context of SSI, describes the data flow between issuer and holder or holder and verifier.
Privacy by design	Design principle according to which data protection and in particular data minimisation are ensured by the conceptual design. In this way, trust can be created without having to establish security through a legal basis and the associated controls.
Public key directory (PKD)	Central register in which the public keys of issuers of proofs are stored. In hierarchical PKI 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.
Registry	Term in the SSI context: Publicly readable storage with the necessary cryptographic evidence for validity verification of verified certificates.
Relying party (RP)	Analogous to verifier, term in the IdP context: System participants that make use of the e-ID ecosystem to verify identity proofs and utilise the personal data represented by the e-ID.
Revocation list	Publicly readable list of identification numbers of issued but withdrawn proofs and certificates.
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 digital proofs, 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.
Verified 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 verified credential in addition to the actual data.
Verifier	Analogous to relying party, term in the SSI context: System participants that make use of the e-ID ecosystem to verify proofs and utilise the data presented by the users.
Wallet	Software application, often designed as a smartphone app, which stores digital proofs and ensures communication with issuers and verifiers.

Contents

1 Purpose of the document

This target vision for an e-ID forms the basis for discussing the common vision of a governmental, electronic identity (e-ID), its design, the scope of an e-ID ecosystem, and many other aspects. The target vision for an e-ID deliberately refrains from describing and evaluating any ultimate solution. A broad discussion should make it possible to specify the direction for an e-ID. The outcome of this discussion will serve to prepare a policy decision by the Federal Council for a new, governmental e-ID solution.

2 Background

2.1 Popular vote on e-ID Act

On 27 September 2019, a clear majority of Parliament passed the Federal Act on Electronic Identification Services (e-ID Act). A referendum was successfully called against the e-ID Act. The e-ID Act was clearly rejected in the popular vote held on 7 March 2021.

2.2 Motions

Following the rejection of the e-ID Act, six motions with identical wording were submitted on 10 March 2021:[1]

The Federal Council is mandated to create a governmental electronic means of identification to prove one's identity (authentication) in the virtual world, comparable to an identity card or passport in the physical world. The principles of privacy by design, data minimisation, and decentralised data storage (such as storage of identity card data with the user) are to be observed in particular. This e-ID may be based on products and services developed in the private sector. However, the issuing process and overall operation of the solution must be the responsibility of specialised governmental authorities.

The demands of the six motions are:

- governmental electronic means of identification comparable to a passport
- data minimisation and privacy by design
- decentralised data storage
- governmental authorities responsible for issuing process and overall operation

2.3 Clarification of the vision of an e-ID

The ideas about an e-ID are diffuse – everyone currently has their own. This document aims to encourage a consolidation and further development of the underlying vision. One goal is to clarify whether an e-ID should also be useable in the physical world (analogous to digital vaccination certificates), whether the e-ID could be granted the same probative value as physical identity documents, and whether an e-ID should be an authentication factor as part of a national, governmental login.

[1] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20213129

The core task of an e-ID is proof of identity by digital means. The e-ID can thus be understood as an "identity card", and a login as *one* possible application of an e-ID. Additionally, the state takes on the role of issuer and operator. This would give rise to the following definition:

"An e-ID is a digital identity card issued by the state, serving as proof of one's identity."

So as not to define the vision too narrowly, this document links the idea of an e-ID directly to the vision of a digital trust infrastructure for Switzerland, which could, for example, be formulated as follows:

"Switzerland has a state-operated digital trust infrastructure which enables and promotes secure processes without media discontinuity."

A governmental e-ID could make an important contribution to such a digital trust infrastructure, but the realisation of that infrastructure would require more (see Chapter 2.4). Eligible persons for an e-ID are understood to be – as already set out in the e-ID Act – Swiss nationals as well as foreign nationals with an identity document recognised in Switzerland or a valid legitimation card, hereinafter referred to as "users". Legal persons always act through their corporate bodies, i.e. natural persons, and therefore cannot be the holder of their own e-ID. They are identified by a uniform business identification number (UID).[2]

2.4 Demands on digitalisation

Digitalisation efforts are often subject to high demands and at the same time a very wide range of expectations and ideas. Technology is no longer perceived as a limiting factor in data and media transmission: "Technically, almost anything is possible." However, a lack of physical tangibility sometimes makes a common, uniform understanding of fact patterns, functions, and roles difficult.

Digitalisation always entails the call to rethink processes and roles. If existing processes are transferred into digital channels without such a review, the result is usually not good digitalisation with efficient digital processes. Ideally, previously necessary analogue process steps can be eliminated. Automation, combined with digitalisation of processes (meaning that the processes are also redesigned according to digital principles) will lead to resource savings, enabling a high level of scalability of the system, which can handle much larger volumes with almost identical resources at a higher quality and speed.

Users must be placed at the centre of development. Users should not be deemed to include only private individuals, but also users from the business sector (acting on behalf of their companies), which can benefit even much more from digitalised processes. Good digitalisation therefore directly improves the conditions for conducting business, processes can be simplified, and the private sector can in turn offer new opportunities for users. In this way, the entire national economy of Switzerland can benefit.

The call for a governmental e-ID can be understood as an assignment of responsibilities to the federal government. The precise powers of the federal government and, accordingly, the possibilities of advancing digitalisation by means of governmental digital infrastructure must still be examined in greater detail, however. It must be borne in mind that the e-ID is not the miracle cure that many are waiting for, hoping that it will solve all digitalisation problems. The e-ID will not digitise Switzerland, but it will support further digitalisation because it is an important infrastructure component of Switzerland.

[2] see https://www.bfs.admin.ch/bfs/en/home/registers/enterprise-register/enterprise-identification.html

Finally, it must be pointed out that many demands are in tension with each other; this means there is not simply *one right way* to do things, but instead a consensual path must be found in the course of the debate, i.e. with respect to the tensions between:

- User friendliness ↔ data protection ↔ data security
- Own responsibility ↔ possibilities for support
- User-centric approach ↔ trust
- Controlled environment with difficult access ↔ open system with easy access
- Only a few, controlled use cases ↔ many, uncontrolled use cases
- Speed of implementation ↔ perfection
- Flexibility ↔ protection of users

3 Developments relating to digital identities

3.1 Technical developments

Due to demands for high data protection and decentralised data storage – as are also included in the motions referred to in Chapter 2.2 – a worldwide discussion on the topic of "decentralised identity" has emerged in recent years. This discussion in turn has led to an entire collection of technologies, new cryptographic procedures, and standards that can be used for the purposes of trust systems. Self-sovereign identity (SSI) is currently probably the most discussed approach, consisting of user-centric principles and technological means. The reasons include in particular the simplicity of the concept, the proximity of the technology to physical reality, and its universal applicability.

One technical pillar of SSI technology is public key cryptography, which has already been providing decentralised, technical proofs of origin in the form of certificates (e.g. X.509) for decades. The uses of these certificates include signing data in biometric passports, issuing the COVID certificate, electronic signatures, and establishing protected communication with a website.

Internationally, the trend towards e-IDs can be seen on smartphones, given that the spread of smartphones is now very high. Solutions formerly developed with chip cards are being replaced by smartphone-based solutions. Digital wallets for storing decentrally managed digital proofs are also at the top of the digital agenda in the European Union. However, the fact is that many e-ID solutions in Europe are currently still "classic IdP" solutions, albeit in many different forms (governmental, private, and federated identity providers).

The new start for an e-ID provides the opportunity for Switzerland to benefit from the latest insights and developments. Because technological development is rapid, a concept is needed that can be implemented in a technologically flexible manner. The aim is to make a conceptual decision. Internationally, the renewal cycles of solutions for digital identities are 5 to 10 years. An ultimate perfect solution will not be possible and should therefore not be strived for. But the goal should be to choose a path that can become the basis for many value-creation processes and promote the digitalisation of Switzerland. The legal framework to be created for a governmental e-ID solution must be designed in a way that is as technology-neutral as possible, explicitly allowing for further development.

3.2 Development under EU law

On 3 June 2021, the European Commission presented a proposal[3] to amend the eIDAS Regulation[4] and establish a legal framework for a European Digital Identity (EUid). If the new regulation is adopted in accordance with the draft, Member States would be required to offer citizens and businesses digital wallets within 12 months of entry into force, in which they can link their national digital identities with proof of other personal attributes (e.g. driving licence, diplomas, bank account, etc.). An EUid is derived from the national digital identity. The wallets can be provided by public authorities or private entities, provided they are recognised by a Member State.

To make the proposal a reality as soon as possible, it is accompanied by a Recommendation. In it, the Commission invites Member States to establish a common toolbox by September 2022 and to start the necessary preparatory work immediately. This toolbox must include the technical architecture, standards, and guidelines for best practices.

The framework established by the Commission is technologically neutral but based on the principles of self-sovereign identity (SSI). The Member States will negotiate the technical standards themselves starting in September 2021. So that the future Swiss e-ID can be notified under the eIDAS Regulation, it is advantageous to be guided by the framework set by the Commission.

4 e-ID ecosystem

4.1 Becoming part of everyday life

All initiatives to successfully introduce a national electronic identity always struggle with the chicken-and-egg problem: Without e-ID, no use cases are created, and without use cases, no e-ID is needed. For that reason, the European context not only builds on the use of an e-ID for eGovernment services, but also relies on secondary applications such as electronic signatures and e-banking access in order to promote dissemination and frequency of use. The value of frequency of use is that it improves mastery of use, expertise, and the chance of becoming a habit among the general public.

If the goal is to allow for the greatest possible number of uses, a functioning ecosystem is required: A jointly used infrastructure with jointly defined rules and many possibilities for a wide range of participants within the system. In the ideal case, the e-ID would therefore function in an ecosystem that has open and standardised interfaces and coordinated governance, does not maintain bureaucratic, inhibiting regulations, and enables practical, automatable updating of e-ID data. This would also create the basis for companies in the private sector to join the ecosystem and develop new processes and business models for it – and in that way to make additional uses possible. As soon as practical uses exist and individual benefit is recognised, this will also awaken the interest of potential users.

User friendliness and satisfaction should also be taken into account as important criteria. Interactions within the ecosystem using the e-ID must be convenient, transparent, yet

[3] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

[4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

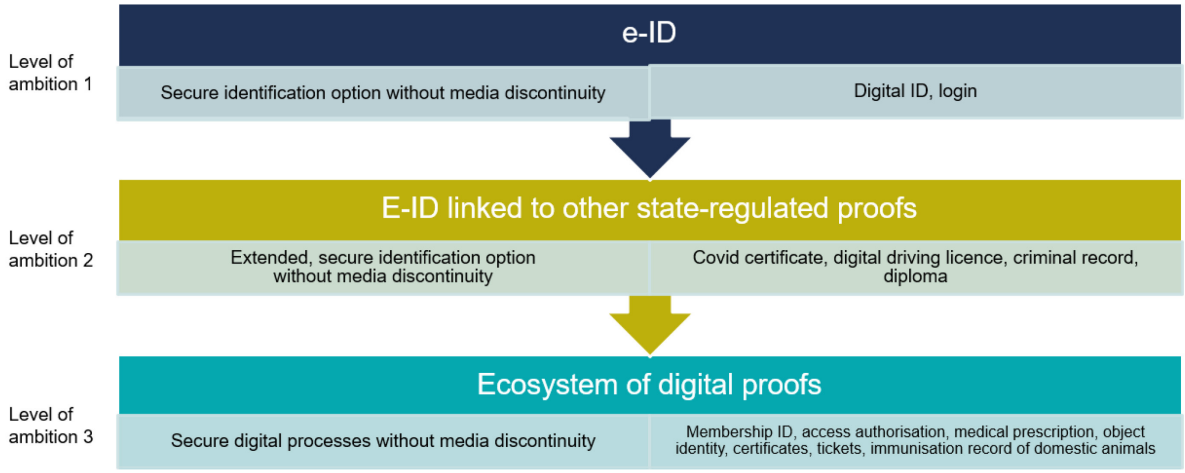
understandable. At the same time, there must be a basic trust in the system, the participants, and the probative value of the e-ID. Use of the e-ID should accordingly not require any additional technical devices. Use of the e-ID would presumably have to be free of charge for its users, given that even small amounts can have a deterrent effect. Barriers to entry should be deliberately kept low. And finally, the e-ID must fulfil the protection and security expectations of everyone involved.

Is that enough for the e-ID to become part of everyday life? Is it enough to build the e-ID ecosystem around an e-ID, or should the scope of the ecosystem be larger, making the e-ID just *one digital proof* among many? The following section addresses this aspect.

4.2 Scope of the ecosystem

Before looking at technological considerations, it also makes sense to think about the question of the scope of future e-ID use ("levels of ambition") and accordingly the scope of the ecosystem. There are interactions between the levels of ambition, the development and design of the ecosystem, and technologies that can be used: The choice of technology should in principle depend on the desired outcome, but at the same time it is important to know that different technical implementations of similar complexity make different outcomes possible.

Following the discussion in the EU,[5] three levels of ambition are defined as a basis for discussion:



Level of Ambition 1: e-ID

Level of Ambition 1 represents the minimum purpose of an e-ID: The e-ID is an identity card that can be used in the digital world to prove one's identity. Only the federal government acts as issuer. The e-ID could be supplemented *by a* login or used *as a* login. The direct benefit of an e-ID as a digital means of identification exists in principle in the following use cases:

- Confirmation of identity (e.g. bank account, mobile phone subscription, ordering of criminal register extract, postal counter, checks of persons)
- Confirmation of age (with derived attributes)

[5] The EU also defines three levels of ambition for the EUid.

The experience gained from the vote on the e-ID Act gives rise to the impression that the benefit of these use cases was not thoroughly persuasive.

Level of Ambition 2: e-ID linked to other state-regulated proofs

Level of Ambition 2 aims at an e-ID ecosystem in which the governmental e-ID represents a basic identity on which many other state-regulated proofs are built, such as the digital driving licence. Here, the basic identity provides personal information such as name, date of birth, and facial image. The driving licence supplement would only need to add the additional attributes such as vehicle category and validity date.

Cryptographic links would create a dependency on the basic identity. Using logical links, an additional governmental proof could also function on its own and would not be affected if, for example, the basic identity had to be revoked.

Compared to Level 1, the scope of the ecosystem would be significantly larger, with a much greater number of possible uses. A wide range of governmental actors would be authorised as issuers, which would also guarantee the correctness of any links.

Level of Ambition 3: Ecosystem of digital proofs

Level of Ambition 3 offers the greatest potential to solve the chicken-and-egg problem. As part of the full scope of the ecosystem, the e-ID would be only one of many digital proofs. A link to the e-ID is possible, but a digital proof can also be independent of the e-ID, e.g. an event or public transport ticket, a membership card, a pet vaccination record, a vehicle registration card, or certification of a successful motor vehicle inspection.

At Level of Ambition 3, governmental and private bodies can issue digital proofs. The ability of private parties to issue such proofs is crucial, given that proofs issued by private parties to other private parties account for a significant number of everyday use cases. This means that many processes can be implemented without media discontinuity using standardised means, e.g. in customer, supplier, and employee management and wherever identification cards, documentary evidence, and certifications are involved. The advantage for the user is that the application (receiving, storing, presenting) is always identical, helping to establish a collective understanding of digital proofs. In the ecosystem, the focus is no longer on the e-ID, but rather on a state-regulated and secured, decentralised repository, "the governmental wallet", from which information can be obtained with a high level of trust.

For the EUid, the EU favours the full option of Level 3, a "highly secure personal digital identity wallet".

The e-ID is indisputably a core element of such an ecosystem, in which the e-ID could support the development of an open, national, digital trust infrastructure. A development in stages is possible in principle in this regard, but the final level of ambition should be defined at the outset, given that not every technological approach is suitable for an open ecosystem of digital proofs (Level of Ambition 3). Each level of ambition can be implemented with one or several technologies. Each implementation entails different consequences. Before describing possible approaches to solutions, however, it makes sense to describe some example use cases in the following section.

4.3 Use cases

To compare approaches, different use cases are described in this section by way of example. For each use case, the current and a possible target state are outlined. Each use case is exemplary for a certain type of application and therefore focuses on specific aspects which should help to raise further questions for discussion.

This listing of use cases does not claim to be exhaustive. Given the need to examine the benefits for citizens, it is crucial to carry out a search for relevant use cases and their evaluation from the perspective of optimal benefit for the user. As already explained above, this consideration will not be conclusive at any given point in time, but must be learned as the use cases evolve. Accordingly, depending on the level of ambition, controlled agile processes must be established that make this possible. Here, the state – as also demanded in some of the motions – has the role of a proactive enabler.

The purpose of the use cases is to demonstrate and examine, by way of example, the direct, concrete benefits for e-ID users. Always implicitly underlying this is the possibility of simplifying processes, resulting in an indirect benefit for the users, whether through faster procedures, less expensive services, or new services. Depending on the level of ambition, service providers themselves (also referred to as "relying parties") may serve not only as recipients and verifiers of proofs, but also as issuers of proofs.

Many discussions of this topic make it clear that there is *no one single use case*; it's the sum and the diversity of the use cases that make the difference! The higher the level of ambition, the higher this sum and diversity will be. Switzerland's innovative private sector could significantly increase this sum and diversity given an open "ecosystem of digital proof" – thus making the chances real of becoming part of people's everyday lives.

4.3.1 Age verification in the analogue and digital world

Age verification involves determining whether a person has reached a certain age. The exact age as well as the date of birth are irrelevant. The e-ID benefit for the user lies in the simple, data-saving application, which is possible in both the analogue and the digital world.

Current state in the analogue world, e.g. entering a disco:

- Security staff check physical identity papers at the entrance to the disco to determine whether someone is, for instance, already 18 years old and accordingly entitled to enter.
- The identity papers include data such as the facial image, the exact date of birth, the full name, and the nationality.

Current state in the digital world, e.g. e-commerce shop:

- In many cases, age verification is omitted and users are asked to declare their age themselves. Such measures do not prevent minors from purchasing articles that are not permitted for their age.
- Verification using photographic or video proof of an identity document requires a fair amount of effort and is accordingly required only rarely.

Focus on the following aspects:

- Age verification using an identity document does not offer data minimisation.

- Marginal data that may be generated during verification processes.
- Insufficient protection of minors due to technical complexity.

Target state in the analogue world, e.g. entering a disco:

- An e-ID can be used in the physical world in the same way as existing identity documents.
- Only two pieces of information are needed for age verification of a person: "Confirmation that the person is older than required" and the facial image. It must be possible to derive this information from the governmental e-ID and provide it for verification without disclosing any further data. Protection against unauthorised further use of the facial image is governed by the Data Protection Act.

Target state in the digital world, e.g. e-commerce shop:

- Issuer of the e-ID does not find out when the e-ID is used.
- For reliable age information, the query of the e-ID information "Confirmation that the person is older than required" is integrated as a process step, similar to a payment transaction.

Concrete benefit for e-ID users:

- Name and date of birth do not have to be disclosed, which ultimately contributes to overall security.
- No physical identification document needs to be carried when entering a disco.
- The protection of minors is strengthened for online purchases.

4.3.2 Opening bank accounts

Hardly any other area is as heavily regulated as the financial sector. Opening a bank account is accordingly subject to many laws and other regulations. It is necessary to have a high degree of certainty about the person who wants to open an account (know your customer). The e-ID benefit for the user lies in the simple transmission of the identity confirmation. In addition, this would make submission of further proofs possible without scanning and sending by email, which is critical in terms of data protection.

Current state:

- Verification of identity on site: presentation of an identity card or passport; a copy of the identity documents is made and kept on file.
- Verification of identity in online processes, e.g. by taking photos of identity papers and subsequent video identification in online processes, which may be partially automated.
- Verification of identity by transferring an amount from an existing bank account held in the same name.

Focus on the following aspects:

- High costs and effort (personnel, financial, technical) needed to implement identification.
- Very high reliability when assigning identity to the holder, so that acts of identity can be attributed to the holder without any doubt (usability as evidence in court).

Target state:

- The e-ID makes simple, secure identification without media discontinuity possible.
- Additional matching processes may still be necessary on the part of the bank due to sector-specific requirements, such as verification of the person in front of the screen by means of a facial image of the digital identity card transmitted during identification.

4.3.3 Debt enforcement register extract

When applying for housing and jobs, an extract from the debt collection register is generally requested. The certification must be obtained from the competent debt collection office. The e-ID benefit for the user lies both in the simple proof of identity when ordering from one of the approximately 400 debt collection offices and in the receipt of a digital debt collection register extract (proof), which can then be presented as often as needed.

Current state:

- First, the competent debt collection office must be found. A search function for that purpose is offered, for example, via the federal government's EasyGov platform, which also provides assistance in filling out a correct request for information.
- Next, the request for information must generally be printed out, signed, and sent by post, together with a copy of the identity card. Depending on the debt collection office, advance payment of the fee may also be required.
- The office sends back a paper extract.
- The user forwards the document (original or copy) to the desired recipients.
- Digital processes are also offered if the person is requesting information for themselves and has a qualified signature, or if the person instructs a third party to obtain the information with proof of interest.
- In these cases, the competent debt collection office sends back a signed PDF. The recipient can check the authenticity of this PDF using a validator application.

Focus on the following aspects:

- Forwarding of extract: The original document is often required.
- Processes on the recipient side are elaborate, given that there is a media discontinuity or a PDF must be checked for valid signature using a validator application.
- Manipulated paper extracts can trick recipients who do not require a recognisable original.

Target state:

- Identification of the orderer can be verified using e-ID.
- The digital extract as proof is sent to the user via a secure channel.
- This digital extract can be forwarded by the user directly to a recipient.
- The recipient system can automate verification processes.

Concrete benefit for the e-ID user:

- The user no longer has to visit the debt collection office or post office.
- The original certification can be presented as often as needed. This means that no additional costs are incurred if the same document has to be submitted to different recipients.

4.3.4 Governmental login

The use of many eGovernment services requires a login to gain access to the platform. A governmental authentication service could be used for authentication, with the e-ID serving as an authentication factor. The e-ID benefit for the user would be the use of the same login data for different eGovernment platforms.

Current state:

- Different IdP or identity management systems for different portals entail a large number of login credentials.
- Many cantons do not yet have identity management for possible eGovernment services.
- No governmental, nationwide login exists.

Focus on the following aspects:

- Make parallel operations possible with existing productive solutions.
- Secure authentication using additional authentication factors.

Target state:

- e-ID represents a (multi-)authentication factor (possession element, possibly also secret knowledge and biometric element).
- A governmental authentication service provides a secure authentication mechanism for all eGovernment portals.
- Identity and access privileges can be separated. This results in considerable simplifications for the design and maintenance of applications.

Concrete benefit for the e-ID user:

- Use of the same login data for different eGovernment platforms
- Secure login process, entailing high access protection

4.3.5 Electronic signatures

Electronic signatures have been governed by the Federal Act on Electronic Signatures since 2005 but have hardly been used by the general public so far. The e-ID benefit for the user lies in simplified access to a qualified electronic signature.

Current state:

- Recognised providers make the necessary services available for electronic signatures.
- The providers first carry out identification of the user; in the case of qualified signatures, personal appearance is required. A qualified certificate is then issued to the user.
- By using a qualified certificate, documents can be digitally signed with legal effect.
- Digitally signed documents can be verified using validator applications.

Focus on the following aspects:

- Cumbersome access to qualified signature due to obligation to appear in person.

Target state:

- Easy access to means of creating qualified electronic signatures.
- Promotion of digital exchange of contract documents.

Concrete benefit for the e-ID user:

- Concluding digital contracts with legal certainty using qualified electronic signatures becomes the norm, saving time and money.

4.4 Legal basis

The analysis of the legal basis of any future act and the preparation of a draft act are not part of this target vision for an e-ID. The envisaged level of ambition and an e-ID solution must first be defined before developing the legal basis for a governmental e-ID.

4.5 Communication

The path to a governmental e-ID requires good communication with everyone from the outset: Potential users, cantons, the private sector, organisations, and the Federal Administration must all be equally engaged with so that they can help to shape and ultimately support the vision. The focus must always be on the potential social benefits, followed by possible use cases and forms of application. Discussions about the technology to be employed follow downstream.

In addition to the usual participation procedures, further voices are to be included where possible via interactive discussion platforms and public intrusion tests.

5 Different approaches to e-ID solutions

5.1 e-ID solution using self-sovereign identity

5.1.1 Approach

Self-sovereign identity (SSI) is the newest approach to an e-ID ecosystem proposed in this target vision for an e-ID. In 2016, Christopher Allen formulated ten user- and data-protection-

centric principles according to which self-sovereign identity[6] is to be defined – identities over which the user has the greatest possible control. This is in line with the zeitgeist, in which topics such as data protection and data security as well as dependencies on central identity systems are increasingly coming into focus, as is also reflected in the motions referred to in Chapter 2.2. At the same time, answers are also being sought as to how systems can be digitally linked to each other in a more universal way instead of always having to define new interfaces.

Within just a few years, open standards, technical frameworks, and a clear architecture for implementing SSI emerged. This did not involve reinventing the wheel, but rather building on knowledge of public key infrastructures and advanced cryptographic methods. This made it possible that productive SSI ecosystems are already in operation today, even though no government so far has issued an e-ID on the basis of SSI. The latest developments in the EU are also moving in this direction.

The SSI approach in principle targets Level of Ambition 3: an ecosystem of digital proof. It is suitable for all levels of ambition, however, given that the technical means are identical – the differences being in governance.

5.1.2 Functional description

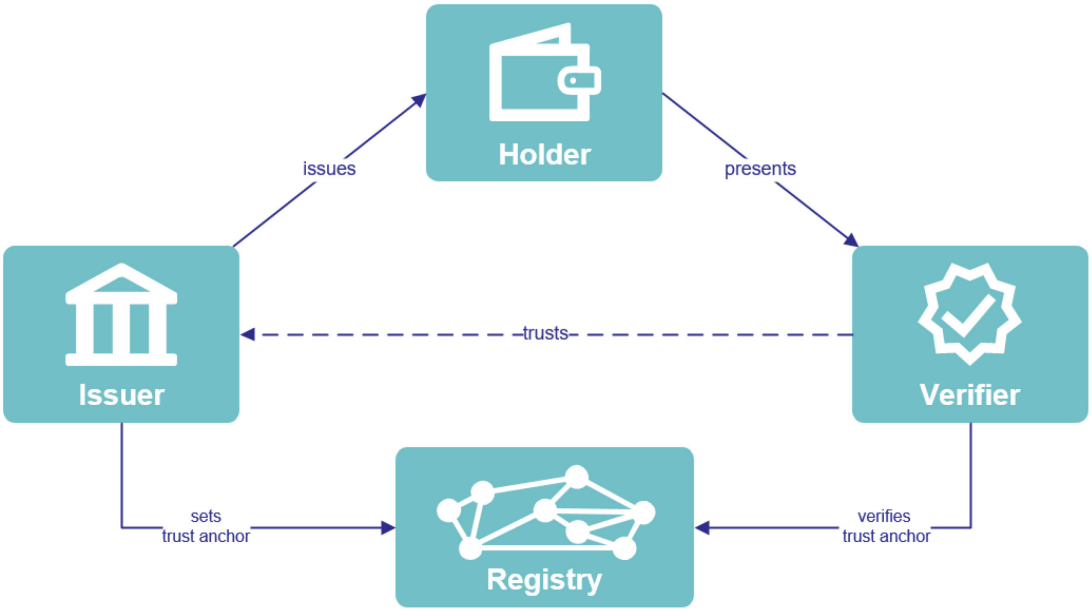


Figure 1: Basic SSI architecture

[6] The term "sovereign" can be misleading, in that a governmental proof of identity is issued by the state and made available to users to be used and managed – the proof of identity is not defined by the users themselves.

The trust triangle consisting of the issuer, the user (holder), and the verifier (relying party) is provided by many trust architectures. The crucial point of SSI is that the links drawn also directly represent the communication flows – without any intermediate instances. The data flow between the issuer and the holder and between the holder and the verifier is performed via encrypted peer-to-peer communication. The communication channel is in general established with the help of a QR code mechanism.

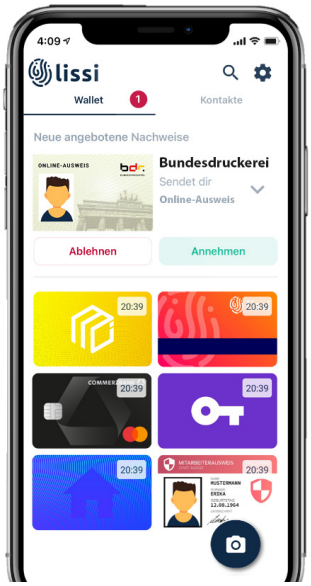


Figure 2: Example of a wallet app used by the holder for receiving, managing, and presenting verified credentials (source: IDunion, lissi)

The issuer transmits verified credentials – i.e. certified digital data – to the holder. The holder stores those verified credentials in a wallet app on a smartphone. Via the secure communication channel, the verifier can request data from the holder. In response, the holder may determine which data is effectively transmitted to the verifier. This data may include verified credentials, parts thereof, or also data entered by the holder.

To verify the authenticity of verified credentials, the cryptographic proofs – not the data itself – are available in a "registry" with electronic trust anchors. As a rule, the registry is a decentralised storage (e.g. DLT, blockchain), in which the issuer has registered its identity and its public keys. Using this registry, a verifier can verify the data presented by the holder without any contact to the issuer and without any third-party instance. The trust relationship between the verifier and the issuer is based either on personal contact or a public reference (e.g. information on a website).

Verified credentials can be defined as "revocable". The issuer then retains the possibility of declaring an issued credential invalid at any time and without contact to the holder. The information on revocable credentials is kept in a revocation list in the registry.

The minimal use case for the e-ID is envisaged as follows:

- The state (issuer) issues the e-ID as a verified credential to the user (holder) in a fully automated process.
- The user manages this verified credential in a wallet app.
- Any third party (verifier) can request the e-ID or parts thereof and check it for authenticity after a controlled transmission released by the user.

5.1.3 Components operated by the state

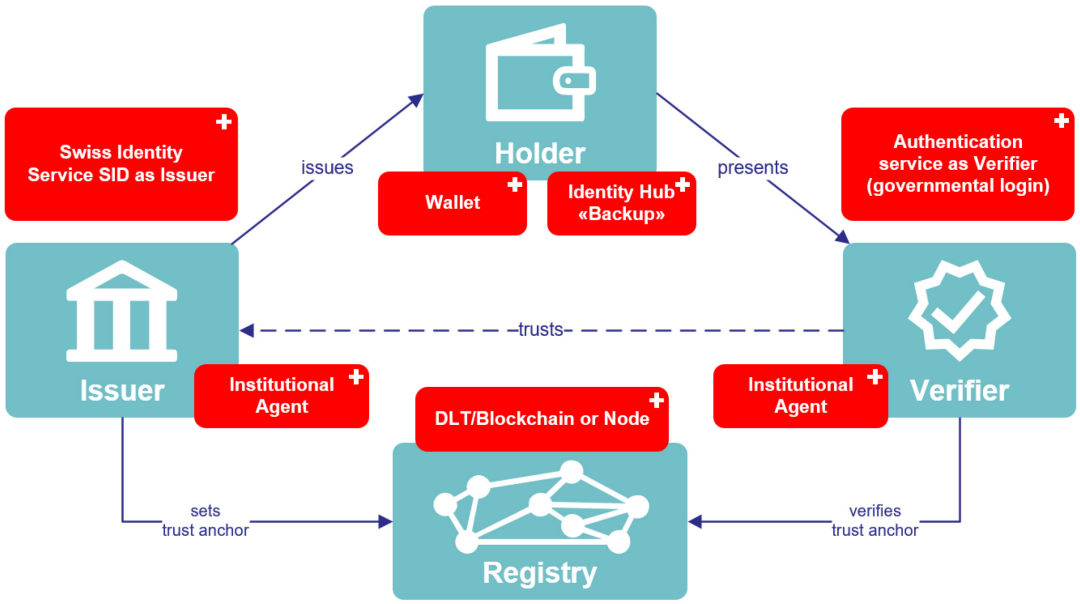


Figure 3: Overview of the components operated or made available by the state (red) in an SSI architecture

Figure 3 shows the following individual technical components in red, which the motions call for the state to operate or to make available as freely accessible software:

- **Swiss Identity Service SID:** Digital, fully automated process for validation, resolution, and verification of a person. The result of the process (with the help of an institutional agent) is the issuance and transmission of a verified credential. This verified credential is the e-ID.
- **Institutional agent:** Software for issuing and verifying verified credentials, providing an API (technical interface) for the complete range of functions.
- **Wallet:** Smartphone application for secure credentials management.
- **Registry:** Data storage with electronic trust anchors, used by all participants in the e-ID ecosystem and generally implemented as a distributed ledger (DLT), e.g. by means of a blockchain. The registry stores cryptographic proofs, identities and public keys of issuers, credential definitions and credential schemes, but never personal or attribute data.
- **Identity hub backup:** Component to facilitate portability and backup of own credentials. An identity hub is not necessary for the minimal functionality of an e-ID but would be recommended for long-term user friendliness and satisfaction in an ecosystem with many credentials.
- **Authentication service:** Login service for governmental and possibly also private platforms. The e-ID credential is used as a (multi-)authentication factor.

According to the demands of the motions referred to in Chapter 2.2, a state authority must be responsible for operating the e-ID solution. The minimal use case should therefore be possible with components created or operated exclusively by the state. However, the technical openness on which the ecosystem is based would allow components to be made available by

private providers as well (especially institutional agent, wallet, identity hub). In the case of the registry, it is possible for the state to provide a part (node) or the entire system – e.g. with the involvement of the cantons.

The SID, IdP, and identity hub components are SSI-external systems that make use of the SSI ecosystem for the issuance, transmission, and authenticity verification of the e-ID.

Standards for interaction are now being developed. This allows the various components to be developed independently of each other and as commissioned by the state. The technical dependencies of the individual elements are limited to the definition of the standards.

5.1.4 Advantages and disadvantages of SSI approach

Advantages:

- The philosophy of SSI is guided by data protection, data minimisation, and privacy by design and meets the demands set out in the motions.
- The generic approach offers many use cases and scenarios, while remaining very close to the physical reality of a "wallet".
- Complete overview for the user of all transactions received and sent.
- International developments are moving strongly in this direction, and many current initiatives and projects are taking this approach.
- Free, standardised interfaces allow third-party systems to be connected.
- Offers a direct, encrypted peer-to-peer communication channel between the parties. In addition to the transmission of credentials, other messages can also be transmitted through the protected channel.
- The basic technologies are open source.

Disadvantages:

- Relatively new approach, some fundamental questions have not yet been conclusively clarified, and standards are not yet complete.
- Broad awareness of the possibilities of this holistic approach (as compared to a login) must first evolve.
- Responsibility for managing verified credentials is transferred entirely to the user, which makes it virtually impossible for the issuer to provide assistance.
- Forensic analysis is difficult because the system is decentralised and cryptographically well protected. If e-ID or other proof is misused, this can make it difficult to prove that "it wasn't me".
- Highly secure wallets for special applications would have to build on secure elements in smartphones. Currently, however, not all smartphones are equipped with these elements, and the necessary developer tools are not yet fully and easily available.

5.1.5 Incorporation of existing cantonal eGovernment platforms

On cantonal eGovernment platforms, proof of identity could be incorporated using the e-ID as a process step, similar to a payment process. Use of the governmental authentication service would also be possible.

A canton could make use of the ecosystem to act as an issuer itself and issue its own proofs, e.g. residence certificates or motor vehicle registration cards. This would also be possible for communes.

In an ecosystem with Level of Ambition 3, in which private sector actors also act as issuers, many other simplifications on the part of the cantonal eGovernment platform would be conceivable: If employers issue salary statements and banks issue interest statements as credentials, these could be submitted directly with the online tax return, for instance, which would simplify the subsequent processes.

5.1.6 Open questions regarding the SSI approach

The core of self-sovereign identity is hardly in dispute in the current SSI community-internal discussions. Discussion points are raised by the proposed approach primarily in regard to governance aspects and SSI-external processes:

- What governance levels are there, and who is responsible for them (e.g. governance levels according to Trust over IP framework: ecosystem, credentials, provider, utility)?
- Does the state have to have a monopoly on certain components? Do wallets have to be certified by the state? Is the choice of wallet and institutional agent left to the user? Are there rules governing which parts are created and operated cooperatively and which competitively?
- Who operates the registry? Is a proprietary national registry necessary, or can an existing international ecosystem be joined? Do cantons, cities, or private companies want to, and should they be allowed to, operate storage nodes? Which technology should be preferred? What role does the data volume play? How can the interoperability issues with other registries be solved? Does the issuer even have the freedom to choose the registry?
- Who is entitled to be an issuer? Does the system remain completely open for the purpose of adding new use cases, or are issuers specifically selected or authorised?
- How are backups and transfers of credentials made possible? How can central backups – which are potentially attractive hacker targets – be avoided? What role does a possible cryptographic connection between the wallet and verified credentials play?
- What security features are necessary for access to the wallet?
- How can verified credentials be used on multiple devices? When would this be necessary? Is it sufficient if one smartphone can always connect to the verifier, even if the user has just used another device to initiate the process requesting the e-ID?
- Who defines credential schemes, is there a need for a certified body to define and coordinate them (e.g. eCH), or are the definitions developed from sector to sector?
- Is there even a need for a governmental authentication service? Would it make sense to combine the issuing process and the deposit of authentication factors in order to

benefit from the complex identification process when issuing the credentials and to enable a high level of security in the authentication process?

5.2 e-ID solution using public key infrastructure

5.2.1 Approach

The state already uses a public key infrastructure (PKI) to secure and validate data in identity documents with a chip (passport, foreign national identity card). The federal government, as the issuer, digitally signs the data before it is stored on the chip and, by publishing the public key, enables all verifiers to validate the data. The technology has been standardised for over 30 years and is used worldwide in a wide variety of technologies. The most recent application of a PKI solution is the COVID certificate.

The PKI approach is similar to the SSI approach. An e-ID issued as a certificate (X.509) is a decentralised identity subject to the full control – and full responsibility – of the user. The user's privacy when using the e-ID is ensured in relation to the issuer, given that the issuer does not know when the e-ID is used. It is much more difficult to achieve data minimisation with this approach, however, since the e-ID is in principle signed as a whole and can therefore only be transferred as a whole to the verifier for identity confirmation.

The approach covers the objectives of a digital proof for analogue and digital uses. Online use of this type of certificate is standardised (mutual TLS authentication). For analogue uses, various procedures based on QR codes have become established (e.g. Swiss Pass in the SBB app, COVID certificate), although no standardisation of offline uses exists.

The generic approach to issuing certificates makes it possible to implement all levels of ambition. Logical or mathematical linking of proofs is possible. The integration of private sector issuers is also technically possible, but the PKI approach is generally only used for issuers belonging to a controlled or controllable group.

5.2.2 Functional description

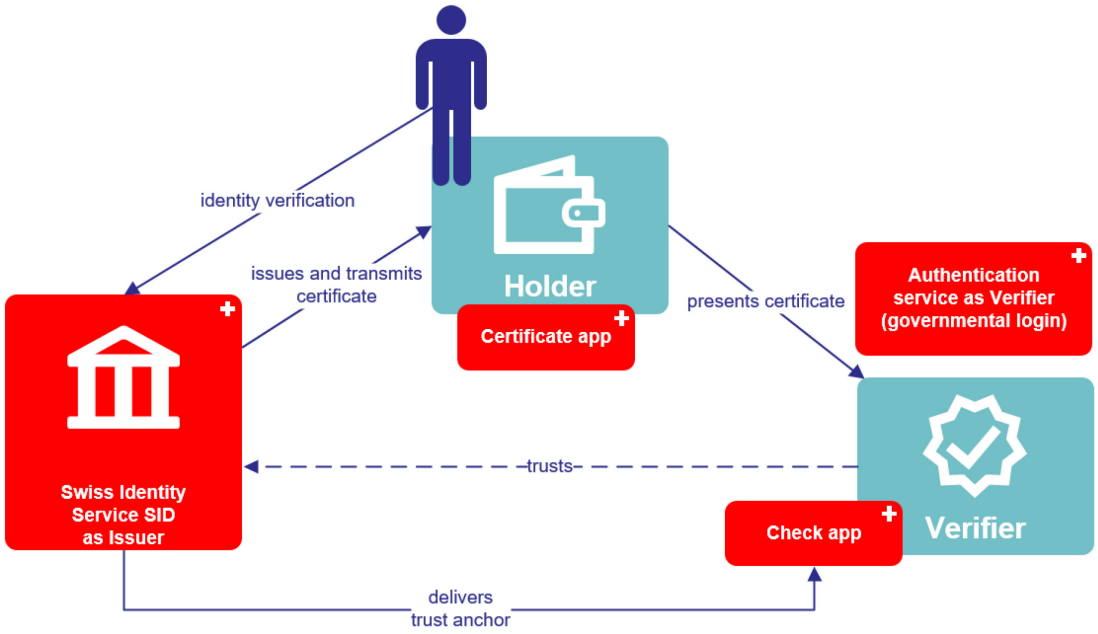


Figure 4: Architecture of a PKI solution

The trust triangle consisting of the issuer, user (holder), and verifier (relying party) exists here as well. The communication flows are as illustrated, but – compared to the SSI approach – different communication channels are possible.

After the identity verification, the issuer issues the certificate and transmits it to the user. The user saves the certificate in a certificate app, which provides copy-proof storage for the certificate. As needed, the user can present the certificate to a verifier via a digital channel or visually via barcode. This discloses all the stored data. After receiving the certificate, the verifier can check the validity of the certificate using the check app. In the check app, the public key of the issuer is delivered directly, allowing verification even at a location without an internet connection.

So that issued certificates can be declared invalid, the issuer keeps a revocation list with all revoked certificates. Various procedures and protocols that strengthen data protection are available for obtaining the revocation list, so that the verifier does not reveal too openly to the issuer when a verification is being performed. The revocation list can be retrieved by the verifier online in real time, periodically, or even decentrally.

5.2.3 Components operated by the state

Figure 4 shows the following individual technical components in red, which the motions call for the state to operate or to make available as open source software:

- **Swiss Identity Service SID:** System for the digital, fully automated process for validation, resolution, and verification of a person. The result of the process is the issuance and transmission of the certificate. The certificate is the e-ID. Additionally, the system maintains the revocation list and makes it available for retrieval.

- **Certificate app:** Application for receiving, storing, and presenting certificates.
- **Check app:** Application for receiving, displaying, and verifying certificates.
- **Authentication service:** Login service for governmental and possibly also private platforms. The e-ID credential is used as a (multi-)authentication factor.

5.2.4 Advantages and disadvantages of the PKI approach

Advantages:

- Use of techniques and technologies that have been tried and tested over many years and are widely used.
- A wide range of characteristics and requirements for the solution can be addressed using this approach.
- The identities and their use are decentralised. No additional marginal data is generated during use. The requirement of privacy by design is taken into account during use.
- Supports the guiding principle of "e-ID is an identity document, not merely a login."

Disadvantages:

- Custody of identities is transferred entirely to the user, and higher reliability for the security of custody and use is almost always tied to additional hardware (e.g. for copy protection or strong multi-factor authentication).
- Certificates can in principle be presented only as a whole. To ensure data minimisation, partial certificates would be conceivable, but the user would then have to apply for and manage several e-ID certificates, making selection of individual attributes depending on the situation cumbersome.
- Different possible transmission channels between issuer, holder, and verifier complicate "proper, secure handling" of the certificates.

5.2.5 Incorporation of existing cantonal eGovernment platforms

On cantonal eGovernment platforms, proof of identity could be incorporated through e-ID as a process step, similar to a payment process. Use of the governmental authentication service would also be possible.

A canton could make use of the ecosystem to act as an issuer itself and issue its own certificates, e.g. residence certificates or motor vehicle registration cards. This would also be possible for communes.

5.2.6 Card-based PKI solutions

A variation on the PKI approach – instead of the certificate app on a smartphone – would be to use a chip card as secure storage for the certificate. A card reader is required for presentation of the certificate – the verifier would have the card reader for analogue uses, the user for online applications. Many smartphone models available today are suitable for reading chip cards. Otherwise, a special card reader is needed.

SuisseID and the new German identity card (nPA) both built on this principle and included digital identification. Both implementations failed to achieve resounding success, with card use as such being only one of the obstacles. Internationally, the development appears to be moving away from e-ID systems with physical chip cards. Future-oriented systems rely on the use of mobile devices/smartphones with special apps, which ensures better adoption mainly thanks to high user friendliness. As an example, the eGovernment pioneer Estonia originally started with a chip card, then introduced a mobile ID linked to SIM cards, and now primarily offers a completely dematerialised app solution (Smart-ID). Germany as well is currently seeking a solution for secure storage of nPA data on smartphones, rendering use of the physical card unnecessary. Switzerland should benefit from these experiences.

Other reasons alongside those mentioned above argue against concrete implementation using a governmental identity card with a chip similar to the nPA:

- While introduction of a new identity card is planned in the coming years, e-ID functionality was not part of the public tender and would have to be procured after the fact. This is also true of identity cards for foreign nationals and diplomats.
- The roll-out of a physical identity document in Switzerland takes at least ten years (plus lead time), given its validity period. Making the adoption of an e-ID dependent on the renewal cycle of the identity card is not conducive to meeting the e-ID's objectives.
- The use of a physical carrier to transmit personal information data limits the choice and possibilities of a future-oriented e-ID solution.

5.2.7 Open questions regarding the PKI approach

- Are application-specific certificates necessary for the e-ID? Could such certificates be limited to a small number?
- What would be the advantages of a public key directory, a management instance for public keys, and revocation lists? How would this change the comparison with the SSI approach?
- Is there even a need for a governmental authentication service? Would it make sense to combine the issuing process and the deposit of authentication factors in order to benefit from the complex identification process when issuing the credentials and to enable a high level of security in the authentication process?

5.3 e-ID solution using a central governmental identity provider

5.3.1 Approach

The failed e-ID Act envisaged a solution with the involvement of recognised identity provider operators from the public and private sector. The idea behind this involvement was that the broadest possible user base would be equipped with an e-ID as quickly as possible and at the same time that use cases would already be available. However, the involvement of the private sector was one of the reasons for the failure of the e-ID Act in the popular vote.

The basic idea of providing users with a state-verified electronic identity based on a login can also be achieved with a central governmental identity provider. Compared to the architecture envisaged in the rejected e-ID Act, this simplified approach would eliminate certain interoperability and data flow issues but would make rapid dissemination more difficult. The

federal government is responsible for operating the system. The solution primarily provides a uniform login for eGovernment services.

The technological foundations and protocols (e.g. OpenID Connect) for this approach are already established and suitable for Level of Ambition 1. Extensions currently under development would be necessary to cover higher levels of ambition.

5.3.2 Functional description

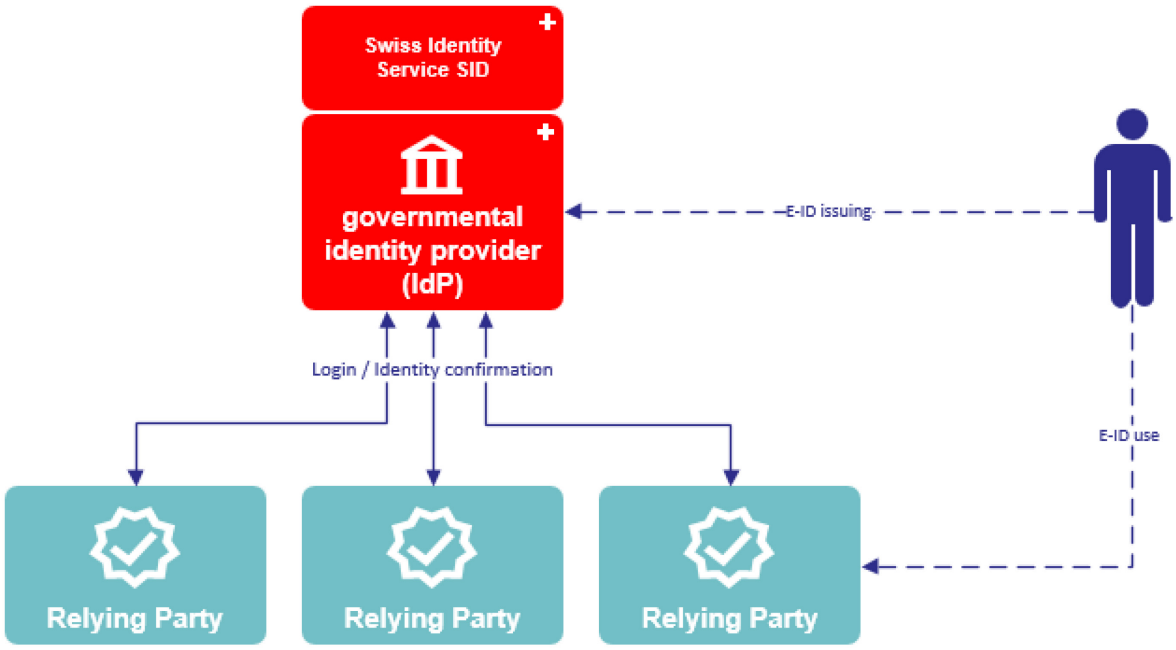


Figure 5: Architecture overview of an e-ID solution on the basis of a central governmental identity provider

At the centre of this approach to a solution is a governmental identity provider. The governmental identity provider maintains the user's e-ID, which can be used in a login process. Any number of relying parties, e.g. cantonal eGovernment platforms, can connect to the governmental IdP. Two options exist:

- The relying party uses the IdP service for active identity management, so that an account login of the user is performed by way of the governmental IdP.
- The relying party uses the IdP service only as a "badge service" where the user can release certain attributes of the e-ID to the relying party in a single process step without the governmental IdP performing identity management.

The user initiates the issuance of an e-ID directly via the governmental IdP. The IdP uses the Swiss Identity Service SID for full verification (see 5.4 Process for issuing e-ID).

In principle, relying parties could offer linked proofs on the basis of a connected e-ID (Level of Ambition 2). An IdP-independent technology approach would be possible, similar to the PKI approach (see 5.2 e-ID solution using public key infrastructure).

5.3.3 Components operated by the state

The small scope of an ecosystem with a central IdP has an impact on implementation. Figure 5 shows the following individual technical components in red, which the motions call for the state to operate or to make available as freely accessible software:

- **Swiss Identity Service SID:** Digital, fully automated process for validation, resolution, and verification of a person. The result of the process is the confirmation transmission of the verification to the IdP for the purpose of establishing the e-ID.
- **Identity provider:** Governmental identity provider (IdP), which manages the e-ID and makes it available to governmental and possibly also private relying parties by way of a login process.

5.3.4 Advantages and disadvantages of the IdP approach

Advantages:

- Simple architecture, clear and comprehensible solution
- Widely used technologies and protocols
- Coupling of personal verification and e-ID login makes it a secure login option.

Disadvantages:

- The solution contradicts the principles called for in the motions. It is not decentralised, and – because the approach is based on complete trust in the IdP – privacy by design is not ensured. The concerns about data economy and marginal data would be mitigated somewhat by the fact that the overall responsibility of the system lies with the federal government, so that close monitoring would be possible.
- Unsolved chicken-and-egg problem: Chances of rapid adoption by users as well as rapid and voluntary linking of many service options are rather low, given the experiences in other countries.
- Limited use scenario, rather difficult use in the analogue world.
- The ecosystem is difficult to expand to higher levels of ambition.
- No separation of issuance of the e-ID from its use. This contradicts current use of identity documents and accordingly does not correspond to the counterpart in the analogue world.
- Linking of the e-ID with other proofs is possible only through the connected services, making the use of these proofs more difficult.
- Does not follow the principle of "e-ID = digital identity card".
- System dependency on an IdP.

5.3.5 Incorporation of existing cantonal eGovernment platforms

The central IdP is connected to the existing cantonal eGovernment platforms. Access and role management would remain with the respective platform, but the identity would come from the federal IdP, which would guarantee a secure login procedure. This could relieve the burden on cantons that do not yet have their own login solution as well as cantons that currently operate

their own IdP. Cantons with existing IdPs could also additionally link the federal IdP to their eGovernment platforms, which in practice means that an identity already existing at the canton's own IdP would be linked to the identity provided by the federal IdP, rather than entailing parallel operation. It should be noted that an architecture using several IdPs is difficult to implement, especially for mobile applications (refresh tokens, etc.). When using a federal IdP for a cantonal platform, due attention would also have to be paid to the issue of support, so that users would have a clear point of contact in the event of problems.

In principle, a federation of already existing cantonal IdPs would be possible. A federation would entail a kind of decentralisation (regionalisation) due to the distribution among different systems. In comparison to a central IdP solution, however, federated systems not only require more resources but also more regulation and control mechanisms (standards, trust level of the identity, data protection, etc.). If additional functions are developed, such as issuance of age certificates, standards would always have to be defined first and then every IdP would be forced to implement this further development as well. Only in that way could all users, regardless of the cantonal IdP, use the same e-ID functions. Despite the reuse of existing IdPs in some cantons, the costs for the state are estimated to be considerably higher than for the implementation of a governmental central IdP that has to be connected to cantonal platforms.

5.3.6 Open questions about the IdP approach

- Who may use the central governmental IdP as a login supplier and to confirm certain attributes? Is the connection reserved for governmental platforms, or is it also available to private sector systems?
- Which eGovernment platforms would connect to a governmental IdP? How many cantons still need an IdP solution at the time of implementation?
- Does outsourcing of the login for cantons and other relying parties even make sense?
- Who is the contracting party in relation to the relying parties, and who is responsible for drawing up the contract? What requirements would relying parties have to fulfil? How is control ensured?

5.4 Process for issuing e-ID

The issuing process for an e-ID is independent of the approach chosen. The following steps are necessary:

- The applicant presents an existing proof of identification.
- The proof of identification is matched with the person.
- The e-ID is transferred to the person by the state.

In the interest of rapid and convenient dissemination, the goal should be a fully automated online process as in Italy, for example. This does not exclude support options at physical counters. The state operates the requisite system and transmits the digital proof to the applicant via a secure channel.

Given the principle that data economy and derived attributes should be possible, the content of an e-ID can be considered in a new light. Attributes do not have to be dispensed with as a precaution on data protection grounds, given that control to pass on each individual attribute lies with the user. The e-ID would integrate the data that is also present on a physical identity

document: given name, surname, date of birth, facial image, place of origin, place of birth, nationality, date of issue. It would also be conceivable to integrate the OASI number, which is required for many official transactions and would therefore be practical for the user.

To ensure a high degree of interoperability internationally, a high level of security should be aimed for when issuing the e-ID (identification and verification). However, the level of security of an e-ID cannot be considered in isolation only with regard to issuance. Different levels of security are possible, depending on the implementation, for the storage and presentation of the proof or when using it through the digital identity card. It thus makes no sense for the discussion to fixate only on a single level of security – the entire chain of trust must be considered for each use case, ideally with a strongly trusted anchor: the e-ID.

The details of implementation of the issuing process must still be worked out and are therefore not covered by this document.

6 Implementation planning

6.1 Timetable

After public debate of the questions raised in this target vision for an e-ID and the evaluation thereof, the Federal Council is expected to make a policy decision by the end of 2021. Based on the specifications of that policy decision, the preliminary draft of the new e-ID Act will be prepared so that the consultation procedure for the act can begin in mid-2022. This is followed by the preparation of a dispatch, parliamentary deliberation, a possible referendum, and the enactment of implementing provisions. The timing of the introduction of a governmental e-ID will depend on this process.

To gain time, it is possible to start implementation planning or effective implementation in parallel with the legislative process. Already during technical implementation planning, initial pilot applications and proofs of concept could be implemented to clarify possible issues in practice. After initial policy discussions in Parliament, tenders and development work could then be initiated.

6.2 Cost estimates for the different e-ID approaches

As is the case with the timetable, there are also many unknowns with regard to cost estimates. A solid estimate is not possible, given that the requirements are still completely open. It can be assumed that implementation of all the approaches presented will be within a similar cost range. Accordingly, a rough cost estimate is not provided at this stage. The costs can be broken down into three areas:

1) Costs for the creation, operation, and further development of the functional and technical systems.
2) Costs for promoting the use and deployment of e-ID by users and the private and public sectors through suitable communication and pilot and support programmes.
3) Costs for ensuring compatibility in the interest of expanding benefits (international, federal, requirements from the private sector).

Naturally, the higher the level of ambition, the higher the costs will be – but this is also directly linked to higher expected benefits.

6.3 Financing options

If one of the main goals is to create a "frequently used platform", state-subsidised funding should be considered: The state would cover the expenses, viewing the platform as a fundamental contribution to the digitalisation of Switzerland. The inhabitants of Switzerland expect a governmental digital identity as a basic service provided by the state.

While this approach does not fulfil the requirement of providing governmental services with fees that cover costs, it does avoid the deterrent of major bureaucratic overhead. If state-subsidised funding is rejected, complex fee models should be avoided so as not to hinder dissemination unnecessarily.

International experiences have shown that users are not willing to pay for an e-ID. The e-ID and use of the associated trust infrastructure must be available free of charge to users.

Regarding the question of which roles could contribute their share to financing, the "verifier/relying party" side is generally omitted in the case of decentralised systems because of data protection precautions. This leaves the issuers, who could – for example under the SSI solution – pay a fee for depositing their own identities, schemes, and credential or revocation definitions in the registry to help finance part of the infrastructure (the actual issuing of a verified credential would be free of charge, given that nothing has to be written to the registry). In the case of an IdP solution, fees could be defined in the usage agreements between the IdP and relying parties.

7 Public debate of the target vision for an e-ID

Even though this target vision for an e-ID contains three approaches to solutions, it is primarily intended as a basis for discussion. Switzerland is facing an important policy decision, and opinions are being sought from the expert public. What does Switzerland want from an e-ID, which ecosystem do users, communes, and cantons as well as the private sector desire, which use cases do users and service providers urgently require?

As a guideline for written comments on the target vision for an e-ID, positions should be taken on at least the following points:

- Where do you see the particular benefit of an e-ID, and which use cases are most important to you?
- In your view, what are the three most important requirements for a governmental e-ID as a digital identity card?
- What benefits do you see in a national infrastructure that enables the state and private parties to issue and verify digital proofs (e.g. e-ID, digital driving licence, employee identity cards, training certificates)?

Of course, additional points can be contributed in the written statements and in the public discussion on any other aspects concerning the e-ID. Questions should also be asked and approaches called into question in the debate. Public debate is the time for expanding one's perspective, thinking more broadly. Should Switzerland bet on an e-ID solution that has potential, without knowing the precise details? Or is a purely governmental minimal option enough? The debate is intended to provide reference points and answers to these questions.

The public debate will take place through various sounding boards with a wide range of representatives from politics, business, research and academia, civil society, the cantons, and the administration, supplemented by public conferences. The results of the various discussions and the requirements already identified will be compiled and presented to the Federal Council as the basis for a fundamental policy decision. In the end, a draft act capable of securing a political majority must emerge that can be accepted by Parliament and the people.