e-ID IN SWITZERLAND

PUBLIC CONSULTATION ON THE e-ID LAW, LeID

SICPA's response

October 2022

Présentted by:
SICPA SA
AV DE FLORISSANT 41,
1008 PRILLY
Suisse

SICPA

Enabling trust

SICPA

table of contents

1 CONTEXT & OBJECTIVES OF DOCUMENT

At its June 29, 2002, meeting, the Federal Council sent out for consultation a draft federal law on electronic identity and other electronic means of proof (LeID).

The objective of this document is to propose some modification to the draft law and to raise some questions concerning its implementation, the aim being to inform the various stakeholders who are evaluating the impacts on existing digital identity systems and processes.

2 PROPOSAL FOR CHANGES

The draft bill on the e-ID (LeID) provides details of the applications, the need for interoperability with European neighbours (Art19 and Art27) and the division of roles and responsibilities of the Confederation, Fedpol and the Cantons (Art4 and Art8). It is important that the law remains technologically neutral (Art25) to allow for future developments. In our view, the current draft satisfies the legislative requirements that would allow the harmonious introduction of digital identity in Switzerland.

Nevertheless, we would like to raise the following points for further consideration.

2.1 ACCESSIBILITY FOR ALL

The first point, which is related to the very definition of e-ID, is accessibility of tools for every citizen, regardless of age and in the case of disability (societal inclusion). The technologies put in place should benefit everyone and it is important that usability aspects are taken into account by technology and service providers right from the design stage. For example, on 28 May 2019, the government of Luxembourg decided to enshrine such a principle in law[1].

The Federal Office of Justice (FOJ) could guarantee accessibility for all by specifying this principle in the law, which would oblige the various providers to comply with relevant current standards in Switzerland and use all available tools, for example those offered by providers of mobile phone operating systems, to make life easier for people with disabilities. It is also important to consider technological inclusion for people who do not have a mobile phone or smartphone.

2.2 IDENTIFICATION (ART1)

Art. 1, para. 2a states:

> *"Aims to ensure secure identification, by means of an e-ID, between private persons and between private persons and authorities;"*

In order to meet ambition level 3, why not also include legal entities? The e-ID would be a very useful means for companies to securely identify their customers or business partners, for example.

PROPOSAL

a. "Aims to ensure secure identification, by means of an e-ID, between private persons and between private persons and authorities or legal entities;"

[1] https://legilux.public.lu/eli/etat/leg/loi/2019/05/28/a373/jo

2.3 IDENTIFIER CONFIRMATION SYSTEM (ART18 AL1 ET AL2)

According to Article 18(1): *"From the outset, the Confederation is delegated the competence to confirm the identity of federal, cantonal and communal authorities that act as issuers and verifiers. It entrusts an entity within the federal administration with the management and maintenance of the identifier confirmation system. This entity maintains a list of authorities acting as issuers and verifiers which it publishes on its website and updates regularly."* In 2022, Switzerland has 2,145 municipalities[2], more than 570,000 companies and many cantonal services and registers. Within the framework of federalism, decentralisation of the management of issuers and verifiers to the cantons should therefore be considered. Indeed, complete centralisation of this function risks being very cumbersome to manage by the designated administration. It could instead be based on existing systems such as cantonal commercial registers or relevant umbrella associations (banks, insurance companies, etc.). It would also be good to clarify what the conditions are, in particular the financial conditions (Art. 26), to be part of the identifier confirmation system (Art. 28 d).

PROPOSAL

Add to Art. 18, para. 2: "*The Confederation may set up a system for delegating the confirmation of issuers and verifiers to public and private bodies. These delegations shall be secured by an associated electronic evidence system*".

2.4 SOURCE CODES (ART23)

Art23 states that the Confederation will publish the source code of the components of the trust infrastructure that it makes available. In its current form, it seems to make the publication of the source codes of all components mandatory, which could in some cases prove problematic in terms of implementation, licensing or security.

In the draft Federal Act on the Use of Electronic Means for the Execution of Tasks of the Authorities (LMETA)[3], Article 9 para. 1 resolves this uncertainty by formulating this point as follows:

"*Insofar as this is possible and sensible and provided that the rights of third parties are preserved, the federal authorities subject to this Act shall publish the source code of the software they develop or have developed for the performance of their tasks.*"

PROPOSAL

In order to remove any legal ambiguity on this point and to be in line with the draft LMETA, it is proposed, for example, to complete Article 23 in the following way (using the terms of Art 9.1 of the LMETA):

"The Confederation shall publish the source code of the elements of the trust infrastructure which it makes available, insofar as this is possible and sensible and provided that the rights of third parties are preserved."

[2] https://www.agvchapp.bfs.admin.ch/fr/state/results?SnapshotDate=01.05.2022
[3] https://www.newsd.admin.ch/newsd/message/attachments/70501.pdf

3 QUESTIONS

In addition to the points raised in chapter 2 of this document, SICPA has identified some questions related to the practical side of the implementation of digital identity. These questions will no doubt be answered in more specific technical orders. However, they may also influence certain articles of the draft LeID law. A list of these questions is provided below:

3.1 PHOTOGRAPHS (ART2 ET ART4 AL4)

Is a photograph considered as "personal data" according to art. 5.a of the Data Protection Act (DPA)[4] in the same way as a name and surname, or should it be considered as biometric data and therefore sensitive according to art. 5.c.4 of the DPA? If it is considered as biometric data, this would require special treatment in terms of encryption and security. According to art. 5.c.4 of the DPA, biometric data allow a natural person to be uniquely identified and the photo could be considered as such. As a reminder, the photograph is displayed on the personal information page of the passport and identity card in the same way as the surname or first name and in contrast to biometric data which are only accessible by the issuing authority. This is important insofar as the passport photograph, being part of the attributes of the e-ID, would not require any particular cryptographic processing and would therefore be at the same level of protection as the surname, the first name or the date of birth.

As an identity photograph can be exchanged as an attribute and be visible for the purpose of identification during a face-to-face check, in the same way as the name and surname, it seems that this attribute of the e-ID should not be considered as a sensitive element in the same way as biometric data. Also, if compromised, a passport photograph can easily be replaced by another photograph of the holder, whereas biometric data in principle and by definition do not change. It would be advisable to clarify this ambiguity in art. 2 of the LeID.

3.2 REVOCATION IN THE EVENT OF DEATH

Article 5 defines that Fedpol is responsible for revoking the e-ID upon knowledge of the death of the holder. It would be advisable to clarify the process of transmitting the death notification from end to end (e.g. via the AVS number).

3.3 PHYSICAL-DIGITAL EQUIVALENCE (ART9)

The draft law establishes legal equivalence of a state-issued electronic identity and a recognised identity document such as an ID card or passport (Art9) which would cover ambition level 1. This would allow, for example, FINMA to adapt the regulations relating to knowledge of bank account holders in Switzerland and to simplify the processes and user experience in the banking sector. However, this draft only covers the equivalence of the identity document and not all other certificates issued by federal, cantonal or communal authorities to cover level of ambition 2. This may considerably slow down the adoption of electronic identity as it would probably require a change of law for each document. According to Art. 9: "*Any authority or service that performs public tasks must accept the e-ID when it uses electronic identification*". Similarly, all electronic certificates issued by federal, cantonal or municipal authorities should have legal value and should also be accepted as such.

[4] https://www.fedlex.admin.ch/eli/fga/2020/1998/fr

In Luxembourg, for example, the only document that has a physical-digital legal equivalence is the certificate of residence[5]. Only this document can be recognised and used by banks in its digital form, which limits the transition to a digital society. The EU eIDAS regulation is being adapted to address this problem by providing a framework of trust and legal validity of digital identity allowing equivalence of all certificates issued by member states within and across borders[6]. This new regulation would thus avoid the need for all Member States to adapt their legislation to cover the equivalence of all state-issued certificates. As Switzerland is not part of the European Union, this new regulation will not benefit the Swiss legislative framework. The objectives of the LMETA seem to cover part of these needs and it would be wise for this law to be a legal basis for adapting federal and cantonal regulations quickly after the introduction of the LeID.

Furthermore, Art. 1 para. 2.d mentions the standardisation of the e-ID. It would also be necessary to standardise all certificates issued by the state, such as certificates of residence issued by the communes, birth certificates or driving licences. It would be sensible for the definition of these certificates to be regulated by a body at federal level in order to guarantee inter-cantonal and inter-municipal interoperability and equivalence.

3.4 UNIQUENESS OF E-ID (ART5 E)

Article 5e appears to indicate that a person can only have one e-ID. While it is obvious that a person has only one identity, in the physical world it is common for a person to have several variations of identity, such as passport and ID card. It is also not uncommon for a person to have more than one mobile phone. Could each device have a wallet that contains a version of the e-ID?

An important question for technical implementation is what the issued eID credential will be linked to (the mobile phone (e.g. IMEI number), other …)?

3.5 MANDATE (ART 15 AL1)

A related issue is the question of the mandate (Art4 para 2 and Art15). In many cases a natural person may be called upon to act on behalf of another natural or legal person and would need either to hold an electronic certificate belonging to that other person in his portfolio, or at least to have access to the portfolio. This includes the case of parents and their children (<14 or even <18), legal representatives in the event of bereavement or incapacity of any kind, or representatives of a legal person. It is a question of clarifying from the point of view of the law the principle and, if possible, the processes that would govern such cases so that technology providers can respond adequately to this problem. In particular, is it possible for the legal representative (e.g. parent) to hold the eID in their wallet? If so, in the case of parents for example, can this eID be stored with two different people (e.g. father and mother)? Or does the child have to have his or her own phone and wallet, which raises the problem of access to the wallet (Art14)?

3.6 IDENTITY OF ORGANISATIONS (ART15 AL2)

At the same time as the e-ID for citizens, an identity for organisations (legal entities) should be considered. The European Commission is working on this matter because the two concepts of identity are linked, particularly in the case of mandates where a natural person (company representative)

[5] https://legilux.public.lu/eli/etat/leg/rgd/2016/03/29/n2/jo
[6] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

represents a legal person for legal or financial transactions, for example. It is in Switzerland's interest to establish an identity system for organisations in parallel with an e-ID for citizens that is compatible with the schemes set up by the European Commission. In particular, it is necessary to clarify the conditions for using the e-ID in the context of a mandate and to clarify the decentralised role of the cantonal commercial registers in this process.

3.7 IDENTITY OF ISSUERS AND VERIFIERS (ART17 AL3)

According to Article 17(3): "*Verification of the identity of issuers or verifiers is not required before they can use the base register. This would imply a resource-intensive authorisation procedure, which would inevitably lead to an expensive and unnecessary bottleneck. Of course, there is a risk that issuers or verifiers could issue electronic evidence by impersonating them. However, this risk is mitigated by the publication of information on cases of well-founded suspicion of misuse of the trust infrastructure in accordance with Article 22 and excluded by the system of confirmation of identifiers provided for in Article 18. The exclusion of registered issuers or verifiers is not technically possible in the base register, but it is possible in the system for confirming identifiers in accordance with Article 18.*"
On the other hand, Article 7 Paragraph 1 describes the duty of care of an e-ID holder: "*He must take the necessary measures that are reasonably required under the circumstances to prevent any misuse of his eID.*"

The article (Art17 AL3) may prove problematic for citizen trust. Relying solely on the citizen's duty of care (Art 7 para 1) while leaving the door open to identity theft by excluding bad issuers/verifiers only after the fact may hinder adoption of the system by citizens. It is therefore essential that during the verification process, the citizen has a clear and easy way to identify the verifier who is making the request to share wallet attributes. The citizen must be able to easily know whether the verifier is part of the identifier confirmation register and if not, a warning notice must appear. This way the citizen can be sure that he or she is only sharing data with legitimate verifiers.

3.8 VERIFICATION WITHOUT INTERNET ACCESS (OUT OF BAND) (ART18 AL3 ET ART20)

In the real world, i.e. during face-to-face verification, should e-ID attributes and issuers/verifiers be verifiable without an internet network (technological inclusion) knowing that technological solutions make this possible?

3.9 WALLET ACCESS (ART19)

Does the Confederation intend to provide the necessary tools to restrict access to the wallet (e.g. Biometrics, Login/Password, ...)? Following people's response to the Federal Act on eID it would seem appropriate for the Confederation to take on this responsibility and to not use similar functions made available by phone manufacturers or their operating systems, in order to have end-to-end control over security (e.g. via the use of biometric templates).

3.10 SERVICE PROVIDER (ART19)

Will the service provider keep the flexibility to delegate, when this is required, the operation of some parts of the infrastructure to a third party, while ensuring that this third party remains under full control of the federal authorities?

4 CONCLUSION

The Self-Sovereign Identity (SSI) approach has been recognised by many public and private stakeholders as the approach of choice for the transition to digital identity of the future. In view of the market trends mentioned above, the expectations of the Swiss population and the technical constraints, SSI appears to be the most suitable approach to ensure a high level of adoption of eID in Switzerland. Even though it is a new approach and a number of questions remain open, there is a good chance that it will become the next generation Internet identity system. As other countries such as Canada and the United States, and the European Union, are currently conducting similar pilot projects to assess the impact on their existing infrastructure and processes, Switzerland could also be among the SSI pioneers shaping the digital transactions of tomorrow.

The draft LeID law submitted for consultation by the Federal Office of Justice (FOJ) lays the foundation for an SSI-based implementation of digital identity in Switzerland. This draft allows the various state and private sector actors to prepare for the adaptation and migration of existing processes and technologies. SICPA has raised a number of issues that could be critical to the implementation and operational management of this platform in Switzerland. We hope that we can initiate open discussions on these issues and contribute to a successful and smooth implementation of digital identity in Switzerland.

We remain at your disposal to share our experience and vision in this field or for any additional information.

SICPA SA
Headquarters
Av de Florissant 41
1008 Prilly
Switzerland

Tel +41 21 627 55 55
Fax +41 21 627 57 27
www.sicpa.com/contact
www.sicpa.com