procivis
AN ORELL FÜSSLI COMPANY

Bundesamt für Justiz (BJ)
Bundesrain 20
3003 Bern

via E-Mail to: E-ID@bj.admin.ch

October 4, 2021

Procivis' statement on the discussion paper "E-ID Zielbild"

Sehr geehrte Damen und Herren

Dear Sir or Madam

On September 2, 2021, the Federal Office of Justice published the discussion paper "Zielbild E-ID" and invited all interested parties to comment on its content {The literal translation of Zielbild is target image; it means the overall vision or end-goal to be achieved. For consistency reasons, "E-ID Zielbild" is used throughout of this document}. Procivis welcomes this transparent and participatory approach and is convinced that it is an important basis for a widely accepted and trustworthy state E-ID that considers current and future needs of users.

The implementation of the legal, technical, and economic aspects of the future state E-ID will take several years - also depending on the chosen level of ambition and solution approach - and should be approached holistically to exploit the full benefits of a state E-ID. The potential of existing cantonal E-ID solutions, as well as the experience and knowledge that exists at the cantonal and municipal level, should be utilized in this process.

In Appendix 1 you will find our positions on the three questions you posed as well as on other points of the target paper which we consider relevant. In addition, we are attaching our own vision for the development of the future national E-ID in the form of my guest article in the Neue Zürcher Zeitung of September 27, 2021, in Appendix 2 to this letter.

We thank you for taking our concerns into account and look forward to making our contribution in the further stages of the development and implementation of the new E-ID law.

Kind regards,

Daniel Gasteiger

CEO and Co-founder Procivis AG

Appendices as mentioned

Appendix 1 – Procivis' statement on "Zielbild E-ID".

The statement is structured as follows:

1. Procivis' position on the three questions of the discussion paper
2. Assessment of the three levels of ambition
3. Assessment of the three approaches

1. Procivis' position on the three questions of the discussion paper

Question 1: Where do you see the particular benefits of the E-ID and which use cases do you focus on?

For most use cases, an E-ID is only the key with which users can gain access to a service. Therefore, the benefit of an E-ID is directly dependent on the available use cases. An E-ID can also only develop its full effect if the use cases initiated with the E-ID can also be processed digitally end-to-end (without media disruption) and in real time. This is not the case, for example, if a user can log on to a government portal with an E-ID and order a confirmation of residence - but then must wait several hours or even days until employees of the administration have created the confirmation in the form of a PDF from the specialist application and send it.

Experience in EU-countries (and with our customers Canton Schaffhausen and City of Zug) also shows that an E-ID can only develop its benefits if it can be used for transactions with public authorities as well as in the private sector - therefore, at least in the long term (depending on the decision in connection with the ambition levels and solution approaches mentioned), after the introduction of the E-ID in 2026, an open ecosystem must be established through which the private sector can access the state E-ID and its trust infrastructure. Further, the use of the E-ID should be possible from the outset in both exclusively digital (transactions on the internet) and analog situations (for example, age verification in a grocery store).

A central, if not the most important use case for a state E-ID is, as mentioned in the target paper under 4.3.5, simple access to qualified electronic signatures. However, the use case described in the target paper is limited only to the signature of PDFs. When designing a future government E-ID, ideally the technical possibilities which combine the government E-ID with the digital signature (ZertES) should be leveraged. This is currently still regulated separately but enables new use cases which go beyond the signing of PDFs.

Other use cases of a state E-ID that Procivis considers important are:

- **Automated online authentication.** As mentioned in the discussion paper under 4.3.4, the E-ID should serve as a secure login for e-government portals and services. In addition, however, it should also be able to serve - thanks to an E-ID wallet solution based on PKI/QR codes - as automated and password-free access to private sector online portals and processes. Furthermore, thanks to credential-based authentication, such an E-ID wallet solution, significant improvements in the user experience can also be achieved.

- In addition to the "debt registry extract" use case mentioned in section 4.3.3, it would be desirable if all **registry extracts from public authorities could be obtained without media disruption** thanks to the national E-ID - in the city of Zug it is already possible today to order and pay for a confirmation of residence without media disruption and to have this delivered back to the "eZug" app as a PDF signed with an organizational certificate practically in real time. Further, the goal was to enable seamless and standardized transmission of digital credentials from one government agency to another (or to the private sector) under the sole control of the citizen.

- **Private sector use cases.** To help the E-ID achieve a breakthrough, it is imperative to ensure that private sector use cases (such as those mentioned in 4.3.2) can be easily and securely implemented by means of the government E-ID in the medium to long term. This is the only way to ensure that the E-ID is widely accepted.

Question 2: What do you consider to be the three most important requirements for a state E-ID as a digital ID?

Procivis considers the following three requirements for a state E-ID to be a priority:

- **Highest possible trustworthiness**. To successfully establish the future state E-ID among citizens, trust in the E-ID is of central importance. Achieving this requires the following elements:
  - Operation of the E-ID infrastructure by the state in Switzerland incl. transparent governance structures related to the operation and establishment of the E-ID ecosystem (certification criteria / bodies).
  - Absolute focus on data protection, data economy, security and "privacy by design" incl. open-source code of the E-ID technology components (e.g. E-ID wallets)

- **User-friendliness**. A simple E-ID solution that is accessible to all age and stakeholder groups of the Swiss population is central to the success of the future national E-ID. A strong focus should therefore be placed on a user-centric design with catchy, media-interruption-free and self-explanatory E-ID applications. The obvious implementation of an E-ID is therefore a smartphone-based wallet solution that supports the relevant applications (see question 1) from the outset. In addition, it must be ensured that simple back-up/recovery options are available if the smartphone is lost.

- **Interoperability**: To be able to use the Swiss E-ID internationally in the medium term, it is imperative that the development of the solution is based on existing and developing international standards. Developments in the EU (EUid/eIDAS v2, EBSI, ESSIF) and the standards of the World Wide Web Consortiums (W3C) should be considered. Furthermore, existing technical standards for the simple deployment of the E-ID should be taken into account (e.g. ISO 18013-5, OpenID).

Question 3: What benefits do you see in a national infrastructure that enables the state and private individuals to issue and verify digital credentials (e.g., E-ID, digital driver's license, employee ID cards, training credentials)?

The benefits that accrue can be summarized in four broad themes:

- **A national trust infrastructure for the public and private sectors**
  Government and private sector actors today operate a variety of isolated 'IAM and login solutions' with varying degrees of sophistication. As a result, existing financial resources (including tax dollars) are often used to fund duplication rather than innovation. A shared national E-ID infrastructure, which can be used by all governmental and private actors, would allow to reduce duplications, to bundle the existing financial resources and to use them purposefully for the further development of the infrastructure.

- **Reduction of transaction costs**
  Processes without media discontinuity thanks to the availability of digital certificates and proofs and the efficient use of digital signatures between authorities, E-ID users and the private sector can replace many manual processes and thus save costs.

  Examples of such process optimizations are:
  - Automated contract processing without media disruption thanks to widespread digital signatures based on the E-ID;
  - Elimination of visual inspections of digitally submitted documents (e.g., extracts from debt collection registers, university diplomas, residence confirmations, driver's licenses, etc.);
  - Automated proof of age when purchasing age-restricted products online or at self-check-out.

  Calculating savings for such transaction cost optimizations is difficult. Estimates from Estonia can be used as a comparison: Here, the widespread use of electronic signatures alone leads to annual savings of 2% of GDP (source: e-Estonia).

Innovation boost and location positioning
The development of a national E-ID trust infrastructure will lead to new specialized technology applications, which will be implemented by innovative Swiss start-ups and companies, which in turn will lead to new jobs. As a neutral country that enjoys the highest level of trust and is committed to democracy and the rule of law, Switzerland could establish a new technology sector with solutions in national E-ID trust infrastructures, which is a global leader and enjoys a high reputation, like our country's positioning as a leading nation in blockchain and digital assets.

Enabling new business processes / models.
By enabling the linking of previously independent digital proofs, which at the same time can be fully controlled by users (keyword - data minimization when sharing such digital proofs in combination with new encryption techniques such as ZKP), new, innovative and above all user-friendly business processes and models can emerge (e.g. "One-Click contracting" for contracts that require credit or other background checks, e.g., rental housing, employment contracts, etc.). The possibilities for implementing such new business processes are almost unlimited and will automatically bring about innovations in all sectors.

2. Assessment of the three ambition levels

From our point of view - and in view of international developments - ambition level 1 (E-ID) is no longer appropriate and would also call into question Switzerland's competitiveness in the medium term. Should this ambition level be chosen for reasons of a necessary gradual introduction (time-to-market) of the state E-ID, it is imperative that in parallel to the development of the legal framework for such an Ambition Level 1 E-ID, the higher ambition levels are also considered, regarding future governance, technology, and ecosystem issues, to easily enable a future expansion of the law. Furthermore, an E-ID at ambition level 1, especially in combination with the classic IdP approach (as put forward for discussion in the target paper), would already be outdated today and could not meet the minimum requirements demanded by parliament and the people regarding "privacy by design", data minimization and decentralized data storage.

Procivis considers ambition level 2 (E-ID with linkage of further state-regulated evidence) to be the minimum goal. There are already technical solutions on the market today that enable E-IDs at cantonal and municipal level including state-regulated evidence (extracts from registers of authorities) and digital signatures, and therefore this ambition level should also be the minimum target for the national E-ID. Also, just the example with the Covid-certificate has shown that such digital proofs can be easily and quickly implemented and, in the future, also easily integrated into a national E-ID wallet.

The establishment of a sustainably functioning ecosystem of digital proofs (ambition level 3) should represent the actual goal of the development of the future Swiss E-ID. To achieve this goal as quickly as possible, no hurdles should be built into the development of the E-ID law that could impair the emergence of such an ecosystem in the future. In addition to the development of the law and the technological foundations, a start should also be made on convincing all stakeholders of such an ecosystem (authorities at all levels, private sector, politicians, citizens) of the advantages of this approach by means of a consistent communication and training strategy.

3. Assessment of the solutions

Procivis assesses the three proposed solutions as follows:

Self-Sovereign Identity is the approach clearly preferred by Procivis. However, the implementation of the E-ID based on the Self-Sovereign Identity philosophy/technology will take time, as many regulatory, technical, and economic issues still need to be clarified. Nonetheless, work should begin as soon as possible on building the necessary infrastructure (national trust infrastructure), clarifying the governance associated with operating this infrastructure, and establishing the ecosystem (government and private-sector players as well as accreditation bodies for technology providers). In parallel, the existing cantonal and municipal E-ID solutions, which are already based on decentralized E-ID wallet solutions, can be further developed. The goal of the E-ID law must be to be able to seamlessly merge these existing solutions with the national SSI infrastructure in due course. The "E-ID Zielbild" identifies important open questions regarding the SSI approach under 5.1.6. Such questions should be clarified in a practical approach by means of SSI pilot projects.

For more in-depth approaches to the open questions, Procivis also refers to the statement from the "DIDAS" association - Procivis is a founding member of "DIDAS" and has incorporated its SSI expertise into the DIDAS statement.

The PKI - Public Key Infrastructure approach is based on proven principles and technologies and has, among other things, advantages in the area of offline transactions, which are also already well standardized internationally (e.g. ISO standard for digital driver's licenses). In our view, however, the PKI approach is no longer up to date and has significant disadvantages, especially compared to the SSI approach. In addition, this approach would also be only partially compatible with Ambition Level 3, since individual attributes can only be used by E-ID users to a limited extent and important new cryptographic procedures (ZKP, etc.) for achieving the goal of data minimization could not be used at all. This would limit the possibilities for further development and would not provide investment protection for the solution in the long term. Further, international developments are moving away from PKI towards SSI solutions.

NB: In the case of a PKI solution in combination with a physical card as the carrier of the certificate, we would fall back to the E-ID solution ("Suisse ID") introduced by SECO in 2010 or to the approach of the German ID card with E-ID chip functionality. Neither of these solutions was able to gain acceptance due to the cumbersome application of the E-ID (additional hardware / software required for use on the PC).

From Procivis' point of view, the disadvantages of the IdP - state identity provider approach already mentioned in the "E-ID Zielbild" are so substantial that this approach should also not be pursued further. Nevertheless, we would like to go into the most important disadvantages again here: With a central E-ID, the most important demands of the six motions "Trustworthy, state E-ID" of March 10, 2021 - namely "Privacy by Design", data economy and decentralized data storage, can only be implemented to a limited extent.

In addition, if the central IdP were to fail, the entire E-ID ecosystem would be affected and would cease to function. Furthermore, a central IdP-based E-ID can only be expanded to a limited extent and a later transfer to an SSI ecosystem would not be possible, as these are diametrically opposed solutions. The attractiveness of a central IdP for hackers is another criterion that speaks against this approach. And ultimately, the discussion in the EU is clearly moving in the direction of SSI. With a central IdP stand-alone solution, Switzerland would risk that the cross-state use of the Swiss E-ID will not be possible.

Appendix 2 - NZZ guest commentary "The future of the E-ID must lie in self-determination"

Print-Ausgabe: 27. September 2021
Weblink:
https://www.nzz.ch/meinung/die-zukunft-der-E-ID-muss-selbstbestimmt-sein-ld.1643642

After the No to the E-ID, practically everyone agrees on the principles for a new edition: data-saving, decentralized and issued by the state. But that alone is not enough for a sustainable solution.

Daniel Gasteiger

The resounding "No" to the E-ID law in March 2021 has created the opportunity to rethink the topic of electronic identity from the ground up and thus consider the demands of the electorate: the E-ID should be issued by the state and meet the highest standards of data protection.

Privacy by design

Several cross-party motions in parliament are therefore calling for the E-ID to be developed according to the principle of "privacy by design" and for data to be kept decentralized and shared sparingly. Statements by the Federal Council also indicate that the target picture for the E-ID is largely clear. Discussions are currently focusing primarily on how this can be achieved. Classic E-ID approaches are still being discussed, as they were also envisaged in the rejected E-ID law. The state would now assume the role of sole identity provider. In this way, two demands of the electorate can be met: It is a state E-ID, and transactions can be processed more sparingly thanks to a single issuer. A chip-based solution on the identity card also belongs to the classic approaches, although various negative experiences, including those in Germany, will hopefully serve as deterrent examples here.

The classic approaches have one thing in common: that they understand an E-ID as a digital document containing a narrowly defined set of personal attributes - such as name, date of birth and nationality - issued by a single institution - the passport office. This contrasts with self-determined digital identities, in English "self-sovereign identities" or SSIs for short. These understand an E-ID as a highly secure, extensible set of personal attributes and are based on a decentralized network architecture. The self-sovereign identity is held in a digital wallet, which can be found on a smartphone, for example. This approach allows many attributes to be maintained, each of which is confirmed by trusted organizations, such as residents' registration offices, road traffic offices or educational institutions. So, in my wallet, in addition to my name and date of birth, there is also space for my driving license, university diploma, and other attributes. I alone decide with whom I share this information - just as is the case today with physical documents.

Considerable groundwork

The possibilities of the SSI approach are currently causing euphoria in many places. This is understandable given the benefits. However, it must be borne in mind that considerable preparatory work still needs to be done both in terms of the technical infrastructure and in terms of standardization and the establishment of the necessary ecosystem. Fortunately, various efforts are already underway internationally. We should take our cue from them to build up the necessary know-how for our country at an early stage. For Switzerland, it is now a matter of recognizing the spirit of the times and designing the E-ID technology from the outset in such a way that it interacts with future SSI standards. In this way, we can ensure that the regulatory, organizational, and technological investments in our E-ID infrastructure achieve sustainable benefits. The fact that the age of self-determined identities has already been ushered in is demonstrated not least by the canton of Schaffhausen and the city of Zug, which are already offering their population an E-ID based on SSI principles that can also be used intercantonally soon.

Daniel Gasteiger is the founder and CEO of Procivis AG, which developed the technical solution for E-ID in the canton of Schaffhausen and the city of Zug.

Disclaimer: Please note that this document is an unofficial translation of the original German version submitted to the Federal Office of Justice.