

E-ID: The transparent citizen in the cyber world?

Concluding Report | 4th SSF Security Talk of October 2, 2019, Kultur- und Kongresshaus Aarau

Despite differences, the National Council and the Council of States adopted a framework law on electronic identification services (E-ID) at the end of the fall session. However, resistance against the E-ID is growing, and the referendum has already been announced. At the SSF Security Talk in Aarau, the first public event after the passing of the federal law, it became clear: Switzerland still has an intensive and exciting debate on the E-ID ahead of it.

More than 80 interested persons attended the 4th SSF-Security Talk in the Kultur- und Kongresshaus Aarau. The top-class event was opened by Vincenza Trivigno, State Secretary of the Canton of Aargau. In her opening speech, she underlined the importance of digitalization for cantonal administrations and the population's need for 24/7 availability of the public sector. With the aim of optimizing **efficiency, user-friendliness and quality**, the Canton of Aargau has also succeeded in jumping on the bandwagon of digitalization - despite budget cuts. The keynote speeches and the panel discussion made it clear that although digital services are used intensively, trust and transparency on the Internet leave much to be desired. The requirements for an electronic identity (E-ID) are therefore all the higher.

E-ID: High potential for businesses and users

At the beginning Markus Naef, CEO SwissSign Group, described the benefits and application possibilities of the Swiss E-ID. At the same time, he also cleared up four widespread misunderstandings about the E-ID. Markus Naef sees the great advantage of electronic identification primarily in the **high added value and the economic savings** (up to 2-4% of GDP), which have a positive effect on all parties involved. Furthermore, the E-ID also facilitates the daily life of the Swiss citizens through its **simple and secure use**. But Markus Naef also emphasized that "Switzerland is still in the early stages of its digitalization efforts compared to the rest of Europe". While initiatives for electronic identity are on the rise in Europe, especially in Scandinavia, **Switzerland is far behind in e-government**. Markus Naef attributes this fact to the **inefficient application and implementation** of electronic identity. Purely governmental models only work to a limited extent, as experiments in Great Britain and Germany have shown - the penetration and spread of the E-ID among the population is low there.

Weltweit sehen Experten hohe Wertschöpfung für die Wirtschaft dank digitaler Identität.
Vorteile einer digitalen Identität

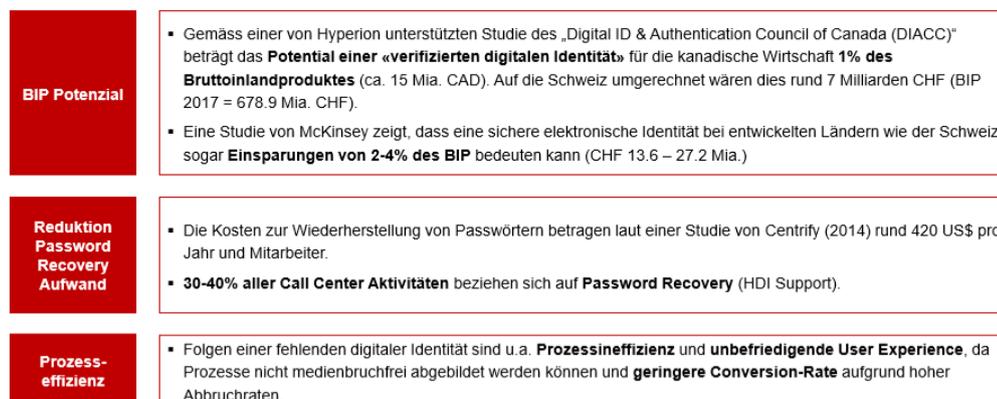


Figure 1: Economic Advantages of an E-ID

Division of labor between the state and the private sector - What role does the federal government play?

An alternative to purely state models is the so-called **Public Private Partnership (PPP)**, which has been successfully introduced in Scandinavia and has proven to be an efficient model. Markus Naef therefore considers it "absolutely necessary" to create a legal basis for a sensible **division of labor between the state and the economy**. This is the only way E-ID systems can really work. Markus Naef welcomes the Federal Law for Electronic Identification Services (BGEID), which was approved in the fall session and defines the state as the issuer and control body of the E-ID and the private sector as the implementing party. In this context, the CEO of the Swiss Sign Group pointed out **four widespread misunderstandings about the E-ID**, which are based on incorrect information and need to be urgently clarified:

- 1) The ID is not issued by private entities, but by the state. Certified private companies only make it "usable in the digital environment".
- 2) No personal data of private persons is collected, evaluated and monetarized. Markus Naef affirmed that Identity Providers (IdP) have no access to the contents of the transaction. Neither identity data nor transaction data are used to create "profiling".
- 3) Furthermore, the E-ID is not a digital passport, which enables border crossing.
- 4) The anonymous use of the Internet is still possible, says Markus Naef. Based on the principle of data economy, identification attributes are not shared for every use of the E-ID.

At the same time, the CEO of the SwissSign Group emphasized that the **federal government certainly does not play a secondary role**. On the contrary, as the issuer of the E-ID, it plays a **leading and extremely important role**. The **principle of subsidiarity**, which is anchored in the present law despite the assumption of a functioning market, is also evidence of this: If the private identity providers do not succeed in developing E-ID systems of the security

levels "substantial" or "high", the federal government would intervene with its own system. Markus Naef is convinced that the division of labor in the PPP-model guarantees **transparency and security**: The customer is at the center and has the freedom to decide which data he or she would like to share.

What is the key to digital trust?

Prof. Dr. Adrian Perrig presented in his keynote mainly the security challenges of the E-ID introduction. As **head of the Information Security Institute** at the ETH in Zurich, he deals with **weak points of digitalization** on a daily basis in order to avoid serious attacks on networks. The ETH professor diagnoses **a lack of trust, sovereignty and transparency as the main problems** of today's Internet. These can lead to serious consequences for private individuals, companies and states, which are always associated with high costs. The basic idea behind Adrian Perrig's research is based on the **transfer of the trust relationship from the physical to the digital world**: A first personal contact or geographical and institutional information should allow the creation of a secure, trustworthy cryptographic key.

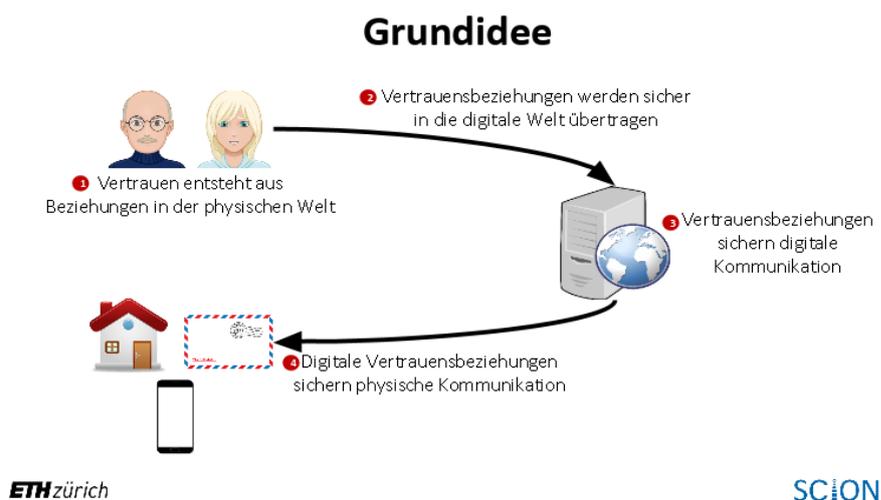


Figure 2: Basic idea – transfer of a trust relationship from the physical to the digital world.

At the same time, Adrian Perrig emphasized that the security thus created can only be verified and guaranteed by a **formal analysis** of the design and mathematical precision. Also, despite advances in research, human error, programming errors, errors in the infrastructure and errors during formal analysis cannot be excluded. Therefore, **error tolerance** must be taken into account already at the planning stage and the number of "use cases" must be increased, explained Adrian Perrig.

Using the opportunities of digitalization

In the ensuing panel discussion, moderated by SSF Managing Director Fredy Müller, the benefits and concerns were highlighted from the perspective of business and politics. While National Councillor Sibel Arslan and National Councillor Beat Flach drew attention to the political aspects of the E-ID debate, Peter Kummer and Roger Keller participated in the discussion as representatives of the business community. The panel was complemented by Adrian Lobsiger, Swiss Federal Data Protection and Information Commissioner (FDPIC).

Peter Kummer, CIO of SBB, is clearly of the opinion that companies must take advantage of the opportunities offered by digitalization in order to remain successful in the years ahead. However, **innovative digital solutions** can only flourish on a secure, trustworthy basis, and the SBB has been able to develop such a basis over the past decades. **Process efficiency** is the keyword that Peter Kummer sees as the main reason for the necessity of an E-ID. **50% of the tickets at SBB today are processed via the Internet and mobile solutions** and this number will increase continuously in the coming years. But also in view of the trend towards more and more digital tickets: The SBB continues to offer its customers personal advice. "Customers can get personal consultations in SBB's more than 150 travel centers and at the most frequented stations," explained Peter Kummer.

Roger Keller, regional manager of the Neue Aargauer Bank, agreed with Peter Kummer: "We are happy to operate counters, not for money transactions or account openings, but to conduct consultations. A successful implementation of the E-ID would be of great interest to the banking world, an extremely security sensitive area. On the one hand, this would increase security and transparency on the side of customers. On the other hand, this would improve the processing speed of banks, says Roger Keller.

Digital education and broad debate as a basic prerequisite for a successful E-ID

Asked how the financial industry is reacting to the **older generation's more negative attitude** towards digitalization, Roger Keller emphasized that the option of payment processing in postal branches will remain. Sibel Arslan, National Councillor for the Greens in Basel-Stadt, agreed with the representatives of the business community that an electronic identity is long overdue and that "hurdles must be removed". However, as a representative of the younger generation of parliamentarians, Sibel Arslan's main criticism is that "we are not making progress in education". The Green National Councillor from Basel-Stadt is convinced that investments must be made in **education and training on the subject of digitalization**, considering the demographic development of the Swiss population. "The E-ID is a must, but with certain criteria" argued Sibel Arslan. Just because time is pressing, no law with obvious weaknesses should be passed. Sibel Arslan emphasized that since the beginning of the discussion, she has advocated a voluntary **choice between a state and a private E-ID variant**. Because the adopted law does not guarantee this freedom of choice, the campaign platform WeCollect has taken up the **referendum**. With the support of the SP and the Greens, the collection of signatures will begin in just a few days. Sibel Arslan contradicted Markus Naef's argument that the referendum

would delay digitalization in Switzerland. As a member of the National Council, she hopes that the referendum will lead to an **intensive, critical discussion between the economy, politics and society**. Sibel Arslan believes that clear answers regarding financing and interests are needed to introduce a successful E-ID.

"Digital Brexit" for fear of attacks on data protection?

Adrian Lobsiger, Federal Data Protection Commissioner (FDPIC), made it clear in his vote that the idea of an error-free digital system is illusory. It is often forgotten that **physical errors are also unavoidable**, emphasized Adrian Lobsiger. Data is processed with human systems and "humans are not perfect beings". Whether analog or digital, the goal is transparency and openness, especially when it comes to identifying possible risks. Adrian Lobsiger also emphasized that the planned independent supervisory authority EIDCOM will have an accompanying, advisory function and will take care of the verification and state approval of identity providers. According to the adopted law, however, implementation is not part of its remit.

Beat Flach, member of the National Council GLP, also advocates **openness towards critical points** of the E-ID. During implementation, the "traceability of activities" is crucial to ensure trust, transparency and security from the citizen's point of view. Although the National Council was not very willing to compromise at the beginning of the E-ID debate, the two councils finally agreed on an **independent supervisory authority (EIDCOM)**. Initially, supervision and verification by the administration's internal information management body was envisaged. However, this body was now deemed unsuitable for this task.

Finally, Adrian Lobsiger pointed out that the discussion on electronic identity is now moving to a **political level**. Although the Federal Data Protection Commissioner considered the political discussion to be positive, he expressed quiet concerns about a possible negative vote. He does not hope that a rejection of the framework law would be interpreted as a "digital brexit".

Tech Giants as Digital Identity Providers

International tech giants such as Google, Amazon and Facebook are growing rapidly and pushing into other areas. Therefore, it seems possible that these tech giants will play a central role in the issuance of an electronic identity even or especially if no agreement is reached in the political process. How can traditional Swiss companies protect themselves from this powerful competition? Peter Kummer, CIO of SBB, made it clear that Swiss companies cannot be left behind and must **increase the speed of digitalization**. Nevertheless, he believes that Swiss companies have a **certain advantage** over tech giants: For the successful dissemination of the E-ID, companies with a trustworthy edge are needed that have a **thorough understanding of the characteristics of the Swiss economy and market**. Beat Flach is also convinced that "we can catch up," although Switzerland is lagging behind in the area of digitalization. This is also where his recently submitted motion on the danger of **digital border blockades** comes into

play: While the unimpeded use of electronic identity in Europe would accelerate the digitalization process, it could also clear the way for tech giants.

Consider the uniqueness of Switzerland

In the concluding round of questions, concerns were expressed about data theft, distribution and monetization of data and financing. How can it be guaranteed that the privacy of identity attributes (such as name, date of birth, gender, place of birth, nationality) is protected when used by companies? Who is responsible if data is nevertheless leaked or misused? How would the costs be distributed if the development of the E-ID fails despite high investments and intensive research?

A key finding of the 4th SSF Security Talk is that **all applications, digital as well as analog, have risks** and are not 100% error-free. The primary goal is to reduce such risks. At the same time, **openness and transparency must have first priority** - especially when dealing with risks and problems that have actually occurred. Whether in the case of a PPP model the costs lie with the state and the profit lies exclusively with the business community will only become clear when the E-ID law is successfully implemented and cannot be predicted based on examples from other countries. Due to its **unique federal structure**, Switzerland cannot be compared with other countries. E-ID models that have been successfully spread e.g. in Estonia or Scandinavia cannot be transferred to Switzerland with a "copy and paste" function. The Discussion has shown that the foundation stone for the Swiss E-ID has been successfully laid. With the referendum there is now the chance to clarify all open questions and concerns together.

In her closing words, Claudia Hollenstein, Vice President of the SSF, thanked the speakers, panel participants and guests for their valuable input and critical questions. She also thanked the event partners, members of the SSF as well as the SSF secretariat, who all contributed significantly to the successful outcome of the 4th Security Talks.

We thank our event partners:

