From SuisseID to SwissID: Overcoming the key challenges in Switzerland's e-credential market

Tobias Mettler
University of Lausanne, tobias.mettler@unil.ch

Ali Asker Guenduez
University of St.Gallen, aliasker.guenduez@unisg.ch

From *SuisseID* to *SwissID*: Overcoming the key challenges in Switzerland's e-credential market

Teaching Case[1]

Tobias Mettler
University of Lausanne
Rue de la Mouline 28
1022 Chavannes-près-Renens
tobias.mettler@unil.ch

Ali A. Guenduez
University of St.Gallen
Dufourstrasse 40a
9000 St.Gallen
aliasker.guenduez@unisg.ch

Abstract

This teaching case explores the political, socio-technical, and business-related challenges of the introduction of a state-recognized electronic identity (e-ID) in Switzerland. Based on real-life events, the case puts every student in the shoes of a board member of SwissSign Group, a joint venture between 20 of the most influential public and private companies in Switzerland. This conglomerate faces three major challenges. To solve these challenges they need, among others, to learn from the past failures of SuisseID, the previous unsuccessful attempt to launch a nationwide e-ID infrastructure. Students must also analyze current political and regulatory events that impact on the e-credential market and need to develop a business model for the new solution, SwissID. This teaching case is designed for students from the undergraduate level upward. The content may be suitable for courses or modules relating to e-government, the platform economy, business models, value co-creation, information ethics, digitalization, PPPs, information security, and privacy.

Keywords: Teaching case, case study, electronic identity, e-ID, digital government transformation

Introduction

Have you been a victim of identity theft? If yes, you are one of several million people a year. Criminals use someone else's personal information to take over existing or to create new bank accounts, make fraudulent online purchases, get mobile phone numbers, or obtain loans or certain government benefits. The numbers are growing significantly year on year, and are starting to take on worrisome proportions. So, what can do about this? Renouncing the Internet and the commodities of modern life is not an option for many if not most of us. The solution to all our current problems is – supposedly[2] – a technological one: electronic identification (e-ID). This is currently seen as a prerequisite for the secure identification, authentication, and digital signing via the Internet (Whitley et al. 2014). Put simply, identification is the process of showing, referencing, or letting know who someone (or something) is. Authentication is the act of proving a claimed identity. A digital signature replaces a handwritten signature. It is used to determine the identity of the signatory of a document in a secure and traceable way. An e-ID brings together all these functions and becomes a key enabler of more trustworthy and more secure private and public digital services (Lentner and Parycek 2016; Melin et al. 2016; Seltsikas and O'keefe 2010).

1 To obtain the Teaching Notes, kindly contact Tobias Mettler.
2 For an interesting article on the black market of fake e-IDs, see Spagnoletti et al. (2019).

In the physical world, identification documents such as passports or (physical) identity cards are ways to provide information on one's identity. In the digital world, by contrast, this function is fulfilled by an electronic identity. Creating such an unforgeable identity is a problem that is as old as computers are.[3] It is frequently reduced to developing systems in a way that they can respond to the following three questions (Fiat and Shamir 1987): First, *Who am I?* This question relates to what experts understand as *identification*. The goal is to recognize an individual by distinguishing him from other persons. Second, *Am I who I claim to be?* This question is associated with what experts call *authentication*. Here, the goal is to verify a person's identity by processing certain data that refer to the person who asks, for instance, something a person knows (e.g. a password, a pin number), owns (e.g. an ID card, a mobile phone), inherits (e.g. a fingerprint, face recognition). The third question is *Can you trust me?* This question relates to the concept of *digital signatures*, which have the goal of creating a certification of the integrity of the person who asks. Encrypting and digitally signing a document provides a strong indication of a person's authenticity and can also be used to detect tampering or forgery of a document during the transmission of a document.

In practice, the implementation of e-ID in different countries takes various forms (see Exhibit 1), and may or may not include all the discussed technological features. Besides these technological differences, there are also different approaches to governance and scaling (see Exhibit 2), as we will now describe.

National e-ID infrastructures in certain countries in Europe

Who has driven the introduction of e-IDs in different countries? Given the interactions between for instance social security benefits, tax returns, casting of votes, many countries' governments have taken leading roles in the introduction of a working e-ID infrastructure (Kubicek and Noack 2010).

A pioneer in and an example of a publicly driven digital identity is Estonia. After gaining independence from the Soviet Union, Estonia already introduced an e-ID in the form of a physical card in 2002 (Martens 2010). Having a digital identity is mandatory for every Estonian citizen, irrespective of their geographical location and their willingness to use the card. Estonia now has one of the most sophisticated card-based e-ID infrastructures in the world; all necessary personal information is stored on a chip. Multiple options exist, such as the classic identity card, the Mobile ID, or the smart ID. The card also provides Estonian citizens with a digital signature. Thus, Estonia's e-ID is not only used as a traditional travel document but also for various other purposes, such as for storing health insurance information, for logging into bank accounts, for e-voting, or as a way to access personal health records (e-Estonia Briefing Centre 2019).

Belgium is another example of a government that has chosen to keep its e-ID infrastructure under its own control. Belgium issued e-ID cards in 2004. There are three types of identity documents: regular electronic ID cards for citizens over 12, kids' ID for nationals under 12, and electronic foreigner cards for both EU and non-EU citizens living in Belgium. Since 2009, all citizens over 15 must carry such a card on their person. Like in Estonia, Belgium's e-ID card is basically a regular ID card with a chip that allows one to perform certain electronic transactions, such as proving one's identity to authorities, signing electronic documents, or securely logging into public digital services. A PIN code gives one access to the secret key on the card (National Register (Belpic) 2019).

Denmark is another example of a publicly driven approach to the introduction of a national e-ID infrastructure. Different to Estonia and Belgium, however, Denmark's government decided to publicly open the process to tender, after an early unsuccessful approach to develop an own solution. Its national e-ID infrastructure, NemID, was launched by a private provider in close cooperation with Denmark's banks in 2010. For Danes, the ID system is free of charge. NemID is a PIN-protected card. Different to Estonia's e-ID, NemID can be used by citizens aged 15 and above, as well as by organizations for public and private services. Its main objective is to offer the simple, secure, and efficient identification of private and public entities as well as to provide a digital signature for documents, particularly for mobile payments (Observatory of Public Sector Innovation 2019).

Sweden's government decided to leave the realization of its e-ID to private sector vendors. Since 1999, mainly banks and large telecommunication providers have offered different e-ID solutions. The first BankID was issued in 2003. The BankID network now includes 11 banks, which makes it one of the most

[3] In fact, the problem is even older; historians found evidence that this was already an issue in ancient Greece.

widely used digital services. BankID is available on several media, including smart cards, soft certificates, and mobile phones. Compliance with the national regulations is monitored by the newly established state agency Verva, which currently is driving major standardization reforms and is creating a more federated approach to personal identification.

In 2000, Germany's government launched a nationwide digitalization initiative that should largely modernize its existing e-government infrastructure. However, this initiative has not yet included a plan to introduce a nationwide e-ID; its major objective was to extend, by the end of 2006, the online presence of public administrations and the availability of public digital services. Not until 2010 was a machine-readable ID card introduced on which all personal information (printed on the card) – and, if desired – fingerprints are stored digitally (German Federal Office for Information Security 2019). In everyday use, the e-ID card can be used for both the authentication and signing of documents. The provision of the infrastructure, hardware, software, and the guarantee of operations was outsourced to the private sector. Owing the low number of public and private services that require e-ID as prerequisite for identification and authentication, adoption of the card has been slow.

As a citizen, you likely access digital services not only from your own home country. Yet, the e-ID infrastructures we have presented above have a strong national focus. To extend the use of locally or nationally issued e-IDs, there is a strong need for an international perspective (see box below).

The European Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

With the goal to establish a digital single market in Europe, on July 2014, the European Parliament issued regulation N°910/2014, which pledges all countries in the European Union (EU) to extend their national e-ID infrastructure so that electronic signatures, electronic seals, time stamps, electronic delivery services, and website authentications work across borders. Electronic identities issued by other countries should receive the same legal status as traditional paper-based documents. This was a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens, and public authorities (European Commission 2019).

The history of the e-ID in Switzerland

"Good things come to those who wait." This expression, used in German-speaking countries, probably best describes the e-ID journey in Switzerland. Known for its low risk propensity, Switzerland's government extensively observed developments in neighboring countries before launching its own e-ID initiatives. Although the necessary legal framework concerning the use of digital signatures was already in place in Switzerland by 2005, it was not until 2010 that an e-ID solution was available in the country.

Initial steps and early failure

Swiss Postal Service introduced, in collaboration with the private company QuoVadis Trustlink, the *SuisseID*, an e-ID solution either based on a USB stick or a chip card. SuisseID had a good starting position. Promoted by the State Secretariat for Economic Affairs (SECO) and financially supported by Switzerland's government with 4 million Swiss Francs (CHF), it was designed to provide a digital signature and an electronic identity to citizens and businesses. While authentication features were mostly requested by online service providers (owing to an increase in online shopping fraud), digital signatures were also demanded by citizens. However, at the time, only the authentication function was offered in the market. To cover the development and maintenance costs, the initial pricing for SuisseID varied for private and business customers, and was between 104 and 363 CHF. The aim was to sell more than 300,000 IDs by the end of 2010. To achieve this goal, Switzerland's government strongly promoted the purchase of SuisseID and granted subsidies to Swiss Postal Service for the ramp-up. But SuisseID did not meet the envisioned target. Although Swiss Postal Service was able to win more online solution providers to invest in SuisseID so as to make the service more attractive, interest from private and business customers was low and mainly related to only one usage case: change of residence. Thus, SuisseID never reached a critical mass and subsequently failed.

Becoming a competitive market

Several reasons led to this failure: For one thing, private customers were not prepared to pay for a SuisseID. Although the initial purchase of SuisseID was subsidized by Switzerland's government, it was fairly expensive to renew, and prices began to rise owing to the absence of a large user base. This led to an exodus of many existing customers. Finally, the solution was simply impracticable. While token-based authentication (with USB sticks or chip cards) were common in the early years of e-banking and e-commerce, in 2013, new competitors such as the biggest telco provider in Switzerland, Swisscom, rushed into the market and offered more convenient solutions, which used only a customer's mobile phone SIM card. Each new SIM card is delivered with the possibility to authenticate. Most importantly, Swisscom's Mobile ID is free to private customers and incurs modest monthly costs for business customers. Another free solution was offered by Swiss Federal Railways (SBB) from August 2015. *SwissPass*, an RFID chip that stores the personal information (e.g. the name, birth date, gender, and photographs) of rail commuters, rapidly became a serious competitor to the two other solutions in the market, owing to the sheer popularity of public transport in Switzerland. Despite criticism from some concerned parties that it allows the SBB to trace citizens' movements, in 2018, around 3.8 million people in Switzerland (44.5% of the population) had a SwissPass (see Exhibit 3).

To increase market penetration, Swiss Postal Service and Swiss Federal Railways started a joint venture in May 2017 with the objective to merge solutions and offer a true, nationwide e-ID infrastructure called *SwissID*. To further extend market power, SwissSign Group was founded in March 2018 – a conglomerate of 19 private and public organizations, including large firms such as Credit Suisse, Raiffeisen, UBS, Axa, Baloise, Helvetia, Swiss Life, and Zurich Insurance Group. Different to SuisseID, SwissID is based on a new business model and is free to citizens. By the end November 2018, more than half a million SwissIDs had already been issued. Numbers will significantly grow when SwissPass and other existing e-ID solutions from member organizations (e.g. banking or insurance ID solutions) will be merged with SwissID in the near future (see Exhibit 4).

A detailed account of events around the introduction of the e-ID in Switzerland

In December 2003, Switzerland's Parliament approved the federal law on digital signatures.

In January 2005, the federal law and related legal ordinances on the use of digital signatures were enacted.

In May 2010, Swiss Postal Service introduced, in collaboration with the private company QuoVadis Trustlink, *SuisseID*, an e-ID solution based on either a USB stick or a chip card. To cover development and maintenance costs, interested users are charged a price between 104 and 363 CHF (including 25 CHF for initial verification), depending on the validity period (max. 3 years). Owing to its high costs, the adoption of SuisseID remained low.

In October 2013, the largest telco provider in Switzerland, Swisscom, launched Mobile ID. Different to SuisseID, it does not rely on an additional token, since it uses the mobile phone's SIM card. It is free to private customers (the use of Mobile ID may incur some fees). Business customers pay a monthly fee depending on the number of e-IDs issued and on usage.

In May 2015, the Federal Office of Police opened an informal consultation, *Concept for Swiss state-recognized e-ID systems*. Switzerland's government decided against a public e-ID infrastructure and restricted its role to defining the legal framework and providing verification of a citizen's identity.

In August 2015, Swiss Federal Railways introduced *SwissPass*, an RFID chip that stores personal information (e.g. name, birth date, gender, and the photo) free to people with a specific commuter ticket. Owing to the sheer popularity of public transport in Switzerland, it quickly became a serious competitor to SuisseID and Mobile ID.

In February 2017, Switzerland's government opened consultation in Parliament for the formulation of a Federal Act on Recognized Electronic Identification Units. The Federal Department of Justice and Police (FDJP) is authorized to prepare a draft version of the law later in 2019.

In May 2017, Swiss Postal Service and Swiss Federal Railways started a joint venture, launching a new, immaterial e-ID called *SwissID*. SuisseID was discontinued. Owing to both public organizations' monopolistic role, this new e-ID solution began to take off.

In September 2017, all major telco providers in Switzerland (i.e. Salt, Sunrise, and Swisscom) support Mobile ID in order to increase its market share and to counter the increasing popularity of SwissID.

In March 2018, Swiss Postal Service and Swiss Federal Railways decided to extend SwissID's reach. A conglomerate of 17 private and public organizations (including Credit Suisse, Raiffeisen, UBS, Axa, Baloise, Helvetia, Swiss Life, and Zurich Insurance Group) founded *SwissSign Group AG* with the objective to making SwissID the de facto standard for electronic authentication and identification in Switzerland. The market power of this new public-private partnership (PPP) is enormous, since it comprises banks, insurance firms, health insurance firms, telcos, and public services.

In March 2019, Switzerland's Parliament votes in favor for the Federal Act on Recognized Electronic Identification Units, with some minor modifications. A publicly owned e-ID infrastructure became a distant prospect. This decision gave SwissID the opportunity to dominate the Swiss e-ID market in the future.

The vision of the future

Can we talk about a truly interoperable, verified, national e-ID infrastructure in Switzerland? As yet, the personal credentials of citizens applying for one of the existing e-ID solutions (e.g. SuisseID, Mobile ID, SwissPass, SwissID) have not been verified by the state. Verification has typically been done indirectly, i.e. a person must submit a copy of an official document as a part of the application process to obtain an e-ID. To develop the necessary legal framework so that issued e-IDs become state-recognized, the Federal Office of Police opened an informal consultation on what will be known as the *e-ID act* (Swiss Federal Office of Justice 2019). This new law foresees a slightly different role for the state compared to the other countries we have discussed. In Switzerland, the state does not act directly as an issuer of the e-ID. Citizens can obtain one through the different e-ID providers without contact with the state (see Figure 1). However, the state provides the relevant and verified information to the e-ID providers that is necessary for e-ID providers to properly authenticate a citizen.

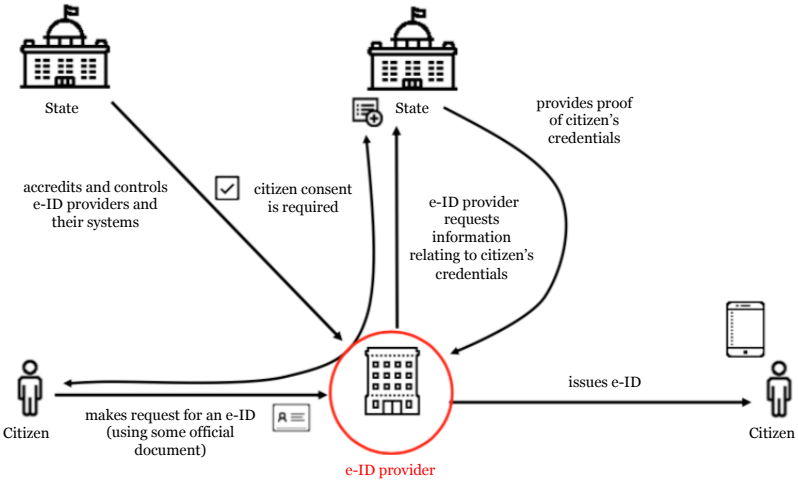

Figure 1. Issuance of an e-ID in Switzerland (based on Swiss Federal Office of Justice)

The state is also not in direct contact with online service providers (see Figure 2) and is not actively involved in the development of the e-ID market. Instead, the state's role is limited to defining the required legal framework, to accredit and control the entry of new e-ID providers, and to oversee the e-ID providers' operations. The latter is subject to a controversial discussion, since it remains unclear how the state can effectively monitor e-ID providers; further, since the state holds equity in all the big players in the e-ID market, some critics fear that it will not be wholly neutral. Another point of discussion is the certification

of e-ID provers. This certification will be optional, but there is hope that this will become an official seal of quality. It is only after receiving certification that e-ID providers become official, state-recognized issuers of e-IDs. In March 2019, Switzerland's Parliament greenlighted the enactment of the e-ID act.

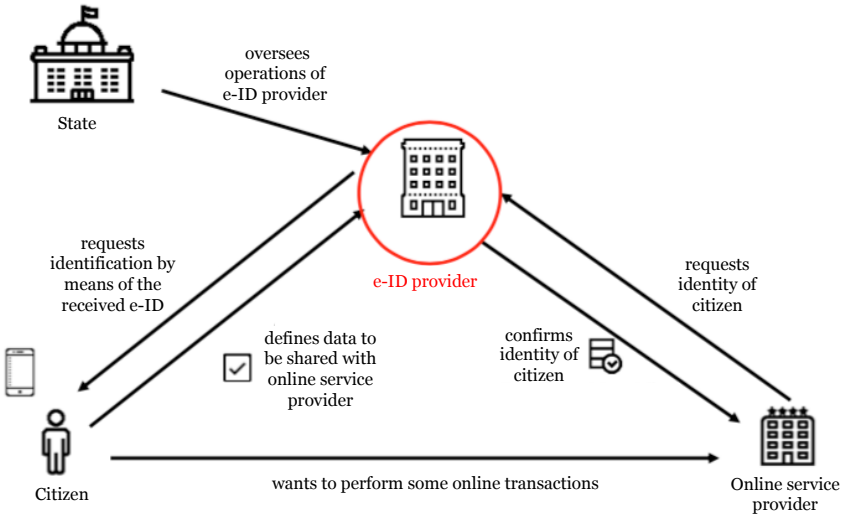

Figure 2. Using the e-ID for online transactions (based on Swiss Federal Office of Justice)

However, as is clear from the previous figures, the state is not the only actor in this e-credential market. More importantly, it is crucial to also focus on the interplays between the e-ID providers, online services providers, and citizens. By understanding this, one may better understand the potentials and perils of the state's decision to not actively seek to develop a publicly funded, national e-ID infrastructure (see the box below).

Actors and their roles in Switzerland's future e-ID market

State: The prevailing opinion in Switzerland is that the dynamic e-ID market is not compatible with the state's fairly rigid architecture. The state is not considered a suitable developer and issuer of the e-ID. Rather, this should be done by private companies. The state must define the rules for the cooperation of all the parties involved in the market, monitor compliance, and sanction misconduct. Thus, the state provides the legal and standardized framework that lays the foundation for trust. Another state function is certification, which is centrally administered by the State Identity Service (SID). Service providers who wish to offer a state-recognized e-ID must first obtain a permit from the state. Once they are recognized as e-ID service providers, the state sends the necessary personal identification data to these service providers.

e-ID providers: The e-ID providers are the issuers of the e-ID. They develop and maintain the technical infrastructure required for the authentication and identification of citizens, ensure the infrastructure's security and operational reliability, and assign and manage personal requests for e-IDs. To be recognized by the state, they must be certified. Although it is voluntary, certification is regarded as a state seal of quality. To activate the e-ID, a citizen first sends their identification data (e.g. social security number and other personal credentials) to the e-ID provider. The e-ID provider forwards them to the SID for verification. The SID then requests permission from the citizen, via the e-ID provider's communication channel, to forward these personal credentials to the e-ID provider. If the citizen allows this, the SID forwards these credentials to the e-ID provider, which activates an e-ID account. Through this process, a citizen can receive an e-ID without any direct contact with the state.

Online service providers: These may be private companies or government agencies that offer digital services that require reliable proof of a citizen's identity (e.g. the passport office, e-banking, secure postal

services, electronic medical records). Online service providers only register an e-ID if they have a user agreement with an official e-ID provider. If there is an agreement between the e-ID provider and online service provider, citizens with an activated e-ID can authenticate themselves in the corresponding digital service. Only if the citizen's given identity turns out to be correct will an online service provider complete the registration.

Citizens: Citizens can apply for an e-ID of their choice. There are only two touchpoints with other actors, mainly with the online service providers from which they request a digital service and with the e-ID provider for the initial registration and the definition of access rights regarding which online service providers are allowed to access what type of personal information.

Challenge 1: How does one deal with the ongoing political debate?

As a *SwissSign Group* management board member, you are in the driving seat and must overcome a number of problems. The retirement and the passive role Switzerland's government adopted have fueled an ongoing public debate, which cannot be swept under the carpet and which has strongly influenced citizens' perceptions of e-IDs generally and specifically SwissID. There is much insecurity among citizens. Many arguments in favor or against the government's decision are discussed in the media. While the number of e-ID accounts is growing, the ambiguity in the public debate may jeopardize active use of SwissID.

What proponents of the future e-credential market are saying

Based on the experiences of other European countries, Switzerland's corporate union, Economiesuisse, argues that a fully publicly funded implementation of a national e-ID infrastructure would lead to a massive explosion of public costs. According to it, a PPP is more cost-efficient and can more flexibly respond to citizens' needs. Some members of larger Swiss banks argue that strong state involvement fosters a monopoly that may hamper the emergence of private and possibly more innovative e-ID providers, limiting "a real choice." The Swiss Trade Association claims that the strength of the outlined e-credential market, compared to a fully public solution, is that it prevents the state from monitoring citizens. In the same vein, most Swiss cantons have promoted the notion that an open market for e-ID providers will lead to more innovative, more flexible solutions, and faster and better adaptation to technological and social changes in the population (the *survival of the fittest* hypothesis). Overall, it is assumed that market competition will generate several user-friendly solutions from different providers, allowing users to choose the solution they trust most. As Swiss FinTech Innovations' members highlight, it is also important to recognize that several private companies have long been working on e-ID solutions. Shifting to a purely governmental solution now would render the resources these companies have invested worthless overnight, "leaving these firms out in the cold." According to them, one must build on already existing efforts. Further, a major assertion is that the majority of (private) online service providers prefer to collaborate with other private entities rather than a government agency. This is important if one is to rapidly and efficiently develop an attractive e-credential market in Switzerland with many online services that require e-ID as a prerequisite. Given that many of the private firms involved in e-ID likely already have established relationships, the emergence of network effects will be achieved much easier and quicker. Finally, the Association of Swiss Cantonal Banks argues that a business-friendly solution will promote Switzerland's competitiveness and innovative strength as a business location, which should be a goal of Switzerland's government, since this is a key strategic objective in the new strategy *Digital Switzerland* devised by the Federal Council.

What opponents of the future e-credential market are saying

Opponents of the direction Switzerland's state has taken have also diffused their arguments in the media. The Pirate Party for instance has expressed strong concerns that private companies will have an incentive to use the data generated during the creation and use of the e-ID for commercial purposes. Although there are legal limits to not exploit the transactional data hosted on private servers, recent cases have shown that private firms don't always respect data protection regulations. Pointing to Sweden's e-ID case, certain cantons have reservations regarding the future interoperability of the different e-ID solutions. In their view,

new e-ID providers have sprung up like mushrooms since Switzerland's government established a legal framework. Thus, it will become more difficult in the future, notwithstanding a major consolidation of players in the market. Certain political parties see the e-ID as a first-order government matter: only the state can really assure a secure and trustworthy e-ID infrastructure. Only by continually testing the security and compliance of the e-ID infrastructure can the state certify and guarantee e-ID providers' quality. But how exactly should this be done? Will the private firms really provide access to all crucial information? Accordingly, opponents such as the Swiss Data Alliance, Swico, and others consider the verification and granting of identity to be the sole responsibility of the state. All parties involved rely on the established identity verification processes of the state. Only the state can offer this trust and reliability; thus, this should not be marketized and left to the whims of market competitors. Further, certain political parties highlight that the credibility of Swiss identity documents is specifically based on the fact that they were issued by the state and not by private companies: "Nobody wants a for-profit firm, such as the SwissSign Group, to have access to very personal medical files, tax returns, and other highly sensitive information just because they issued an e-ID." SwissSign Group needs to devise a communication strategy to counter this and possibly other criticism.

Challenge 2: How does one overcome techno-skepticism?

The ongoing political debate about Switzerland's government's role holds danger for SwissID's future success. As we know from the lamentable fate of SuisseID, technological and economic[4] aspects also critically determine e-ID adoption and diffusion (Wihlborg 2013).

What proponents of SwissID are saying

There are some good reasons for an e-ID. More and more transactions (e.g. electronic payments, online shopping) are done digitally. Once citizens go online, they leave a digital footprint. But most citizens want to retain sovereignty over their data. They do not want to disclose vast amounts of data in every online business transaction, which then can be further used and commercialized. Also, the more you distribute your personal information among different platforms, the higher the risk of falling victim to identity theft. As the proponents of e-ID argue, an e-ID can give citizens back control over their own data. Data security is ensured as follows: The e-ID system can be set up double-blind. This allows e-ID users to disclose only minimum information (e.g. about their insurance cover) as confirmation to other trusted third parties. To do this, an insurance company must be part of the e-ID market (i.e. be a reliable party). If the e-ID holder authenticates themselves on a portal of another reliable party, which needs to know whether a person has an insurance policy, this information can be queried directly via the e-ID. The trusted third party only receives information that the insurance policy exists, but no other sensitive information. Conversely, the insurance company also receives no details about the third party to whom the information was sent. Thus, the e-ID system functions as a kind of data broker, which increases citizens' privacy – both security and comfort increase with the use of e-ID. Users can use their e-ID as their only login. It is cumbersome to have and memorize many passwords and user names. Further, login procedures are both a nuisance and time-consuming. In the case of SwissID, a holder of an active e-ID simply needs to click on the PROCEED icon on a reliable party's website.

[4] The economic dimension is addressed by the subsequent challenge.

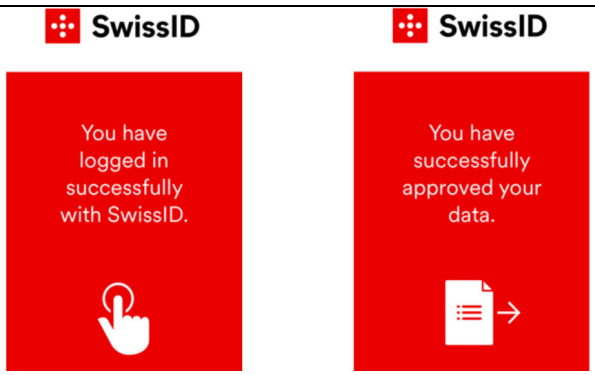

Figure 3. User interactions with SwissID

A digital identity can increase security, trust, and comfort for citizens *and* for online service providers. Without an approved e-ID, it is hard, costly, and time-consuming for an online service provider to effectively establish whether or not someone is who they claim to be. This is a fundamental function of an e-ID. All information in an e-ID is confirmed and verified and is therefore reliable and trustworthy. This allows processes to be carried out online, which previously required high or very high trust in the identity authentication (e.g. tax returns, conclusion of contracts, inspection of pension funds, car rentals, etc.). No time-consuming research and confirmation process is required. This could have considerable cost savings, can increase the conversion rate, and can reduce fraudulent behavior in online shopping, since online service providers may fear misleading accounts or fake addresses less. For proponents of e-IDs, this clearly responds to the need for more secure business transactions owing to the increase in identity theft on digital channels.

What opponents of SwissID are saying

In contrast to the previous arguments, there are many reasons against the national introduction of an e-ID infrastructure in Switzerland. First, having an e-ID is not an absolute necessity. As a SECO-commissioned study showed, there is low public interest in digital signatures and authentication via an e-ID (Hirter et al. 2016).[5] People seem to not have a real pain point, especially because Switzerland's system has strongly fostered trust between citizens and the state. But what if it becomes mandatory to use an e-ID to access certain government services? The so-called *transparent citizen* scenario is one that almost all political parties in Switzerland seek to avoid. Thus, the introduction of e-ID could also be seen as risk for government-citizen relationships.

Opponents of the current constellation also argue that *SwissSign Group*'s dominant role could pose a risk to citizens' privacy. Representing all major banks, insurance firms, and public organizations, there is a certain suspicion that the transactions in this system may be exploited by one or several of the involved parties. As many national and international data scandals have shown, there is a very high incentive (and criminal intent) to somehow further commercialize the data. Because Switzerland's government's governance and control mechanisms are still very vague, many citizens prefer to not actively use their e-ID.

Security experts also point to a single point of failure risk. Since much personal information is stored on e-ID providers' premises, they could become targets for hackers. In this perspective, a distributed solution such as that currently used by users (different logins for different digital services) makes it harder for hackers to access sensitive information.

[5] Note that having an e-ID account, provided to one by default (e.g. SwissPass if you are a train commuter) is not the same as actively using the e-ID for online transactions. We still know very little about the de facto uses of e-IDs.

Finally, if we look at SwissID's positioning, we see even more problems. There are other solutions on the market that are almost instantly available. If you have a mobile phone with a Swiss telco company, you get a Mobile ID. If you have a commuter ticket, you get a SwissPass. However, there is a need to create active demand for SwissID. Further, the benefits to online service providers (e.g. the Swiss online shop Digitec) are limited; in fact, it could even be unattractive to them, because they may lose valuable customer-specific information, which they currently collect. SwissID is based on the standard of minimal information, i.e. when customers order online from these companies, SwissID confirms only that they are of legal age, not how old they are. This stands in contrast to the logic of many of these companies, which use sophisticated data collection and repurposing strategies, to their advantage. Thus, SwissSign Group must identify ways to become more attractive.

Challenge 3: How does one overcome the chicken-and-egg problem?

Switzerland's e-ID market is a good example of a multisided platform that features two (or more) distinct groups of actors who depend on one another. The platform owner (in our case, SwissSign Group) needs to create value in the e-ID market by matchmaking (or building) a user base and by minimizing transaction costs between two or more distinct affiliated actors (in this case, citizens and online service providers). For such an e-ID market to become sustainable, there is a need for a long-term strategic plan in order to balance the involved parties' distinct demands (Vimarlund and Mettler 2017). A market very seldomly emerges spontaneously owing to a shared interest or demand.

However, what interests are more important or should be addressed first, given the limited available resources? Should SwissSign Group intensify its marketing to get more citizens to use SwissID, or is it more important to build a considerable network of online service providers that base their services on SwissID? This problem, commonly referred to as the *chicken-and-egg problem*, is a massive task for all e-ID providers. On the one hand, online service providers don't want to invest in a platform with a weak customer base. On the other hand, citizens are more likely to use SwissID if a large number of leading online service providers use it in their registration process. There is a vicious circle here: the more people have a SwissID account, the more online service providers are likely to integrate it into their digital services; the fewer online service providers are willing to accept an e-ID as a login, the fewer individuals will request an e-ID.

SwissSign Group's managers firmly believe that an ecosystem approach is the best way out of this negative spiral. Their solution is to roll out SwissID to all the shareholder companies in the joint venture. The fact that the conglomerate contains most of Switzerland's biggest companies will make SwissID attractive to citizens from the outset. A first milestone was replacing the old registration procedure of Swiss Postal Service with SwissID. Suddenly, SwissID had several thousand active users, making it more attractive for other online service providers. UBS and SBB are expected to follow. Will this be enough for SwissSign Group to kickstart SwissID and to create lock-in effects?

Tasks for Students

Given the ongoing heated political debate, techno-skepticism, and the challenging chicken-and-egg problem, it is hard to successfully implement e-IDs in Switzerland. It is your job to take over. As a SwissSign Group management board member, what will you do to overcome these challenges in Switzerland's e-credential market?

References

e-Estonia Briefing Centre. 2019. Retrieved April 15, 2019, from https://e-estonia.com/solutions/e-identity/id-card/

European Commission. 2019. Retrieved April 15, 2019, from https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

Fiat, A., and Shamir, A. 1987. "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology,* A.M. Odlyzko (ed.). Berlin, Heidelberg: Springer, pp. 186-194.

German Federal Office for Information Security. 2019. Retrieved April 15, 2019, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper.pdf?__blob=publicationFile&v=7

Hirter, C., Braun, N., Langhart, M., and Gmünder, M. 2016. "Evaluation of project SuisseID 2009-2015," Institute for Economic Studies Basel, Basel, Switzerland.

Kubicek, H., and Noack, T. 2010. "Different countries-different paths extended comparison of the introduction of eIDs in eight European countries," *Identity in the Information Society* (3:1), pp. 235-245.

Lentner, G.M., and Parycek, P. 2016. "Electronic identity (eID) and electronic signature (eSig) for eGovernment services–a comparative legal study," *Transforming Government: People, Process and Policy* (10:1), pp. 8-25.

Martens, T. 2010. "Electronic identity management in Estonia between market and state governance," *Identity in the Information Society* (3:1), pp. 213-233.

Melin, U., Axelsson, K., and Söderström, F. 2016. "Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective," *Transforming Government: People, Process and Policy* (10:1), pp. 72-98.

National Register (Belpic). 2019. Retrieved April 15, 2019, from https://eid.belgium.be/en

Observatory of Public Sector Innovation. 2019. Retrieved April 15, 2019, from https://www.oecd.org/governance/observatory-public-sector-innovation/innovations/page/nemiddanishnationaleidanddigitalsignaturescheme.htm

Seltsikas, P., and O'keefe, R.M. 2010. "Expectations and outcomes in electronic identity management: the role of trust and public value," *European Journal of Information Systems* (19:1), pp. 93-103.

Spagnoletti, P., Me, G., Ceci, F., and Prencipe, A. 2019. "Securing national e-ID infrastructures: Tor networks as a source of threats," in *Organizing for the Digital World*. Cham: Springer.

Swiss Federal Office of Justice. 2019. Retrieved April 15, 2019, from https://www.bj.admin.ch/bj/fr/home/aktuell/news/2018/ref_2018-06-01.html

Swiss Federal Office of Statistics. 2019. Retrieved April 15, 2019, from https://www.bfs.admin.ch/bfs/en/home/statistics/population.assetdetail.7946001.html

Vimarlund, V., and Mettler, T. 2017. "Introduction to the ecosystem for two-sided markets, barriers and facilitators," in *E-health two-sided markets,* V. Vimarlund (ed.). London: Academic Press, pp. 3-15.

Whitley, E.A., Gal, U., and Kjaergaard, A. 2014. "Who do you think you are? A review of the complex interplay between information systems, identification and identity," *European Journal of Information Systems* (23:1), pp. 17-35.

Wihlborg, E. 2013. "Secure electronic identification (eID) in the intersection of politics and technology," *International Journal of Electronic Governance* (6:2), pp. 143-151.

Exhibit 1: The technical implementation of e-ID

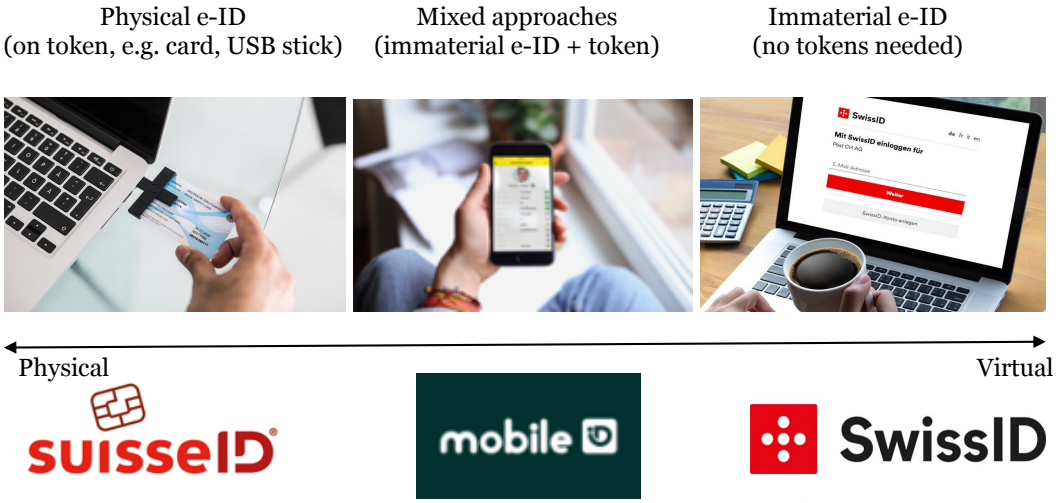

Figure 3. The range of technical solutions for implementing e-ID

Exhibit 2: A comparison of nationwide Swiss e-ID infrastructures

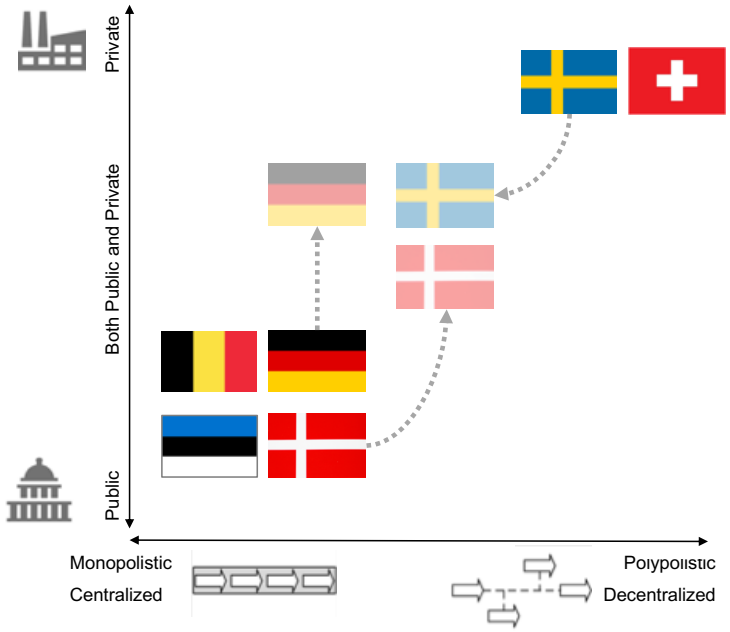

Figure 4. Current state and possible future development of governance and scaling of nation-wide e-ID infrastructures of selected countries (the shaded flag = the future tendency)

Exhibit 3: Overview of market shares of Swiss e-ID solutions

Table 1. Market shares of Swiss e-ID solutions					
Name	*e-ID type*	*Issuing organization*	*Ownership*	*Launch date*	*Approximate number of clients in 2018 (self-reported)*
Suisse ID	Based on USB stick or chip card	Swiss Postal Service	Public	May 2010	270,000
Mobile ID	Based on SIM card	Swisscom (now a joint venture with other telco companies)	Private	October 2013	2 million
SwissPass	Based on RFID card	Swiss Federal Railways	Public	August 2015	3.8 million
SwissID	Virtual	SwissSign Group AG (a joint venture between large private and public companies)	Public-private-partnership	May 2017	500,000

Note: At the end of 2018, Switzerland had a population of 8,542,300 (Swiss Federal Office of Statistics 2019)

Figure 5. Current shareholder companies of SwissSign Group AG