Deloitte.

Digital Identity in Switzerland
A new vision and more agile approach

Table of contents

In its latest global insight on the future of eID, Deloitte discusses new possibilities for public services at the interface of the digital and physical worlds and emphasises the need for a new vision and improved trust in digital identities, or eIDs. Switzerland is lagging behind other countries. But the initial rejection of the introduction of a national eID law by Swiss voters in 2021 also presents an opportunity to learn from best practices and success stories in other countries in order to develop a viable future eID solution.

New digital services often require new forms of identity. For years, governments across the world have been using a patchwork of systems to identify people – for example, physical ID cards like drivers' licences or passports and generic logins and passwords to identify digital users online. There are still only a few solutions that can identify both physical and digital identities to the degree of accuracy needed for public services.
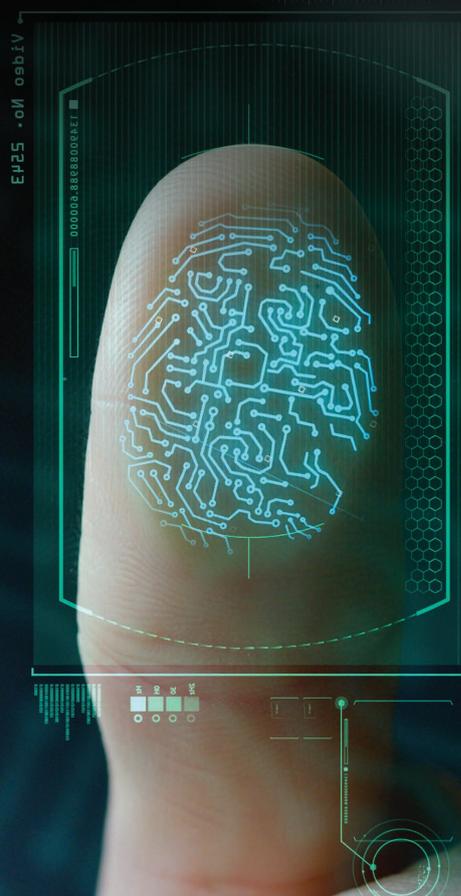
New vision for digital IDs

For future digital services to be successful, a much more agile and user-controlled identity is required. It must enable individuals to selectively manage the exchange of their personal attributes and data while interacting securely with commercial and public services. According to Deloitte's study on the future of digital identity, the ideal solution should have three hallmarks: portability, transparency, and individual choice.

A digital identity needs to work across a variety of platforms and services and citizens should be able to access their identity on a phone, computer or physically. Seamless portability requires a curated ecosystem of issuers and verifiers that follow standards and link to a core identity from a governing authority. With a range of players, transparency about the tools, technology, and methods used to establish identity is essential in order to ensure trust at every step. With transparency also comes the opportunity for users to control their own data – for example, to choose which credentials to use or which data to release. To achieve this level of agile identity, different centralised, federated or decentralised approaches have been implemented with great success in different countries.

International success stories

In Italy, for example, the public digital identity system, SPID, has been offering access to online public services since 2016. The system is made available by several trust service providers (TSPs) supervised by the Agency for Digital Italy and recognised by the EU – in an example of successful public-private collaboration. Adoption of SPID has been fuelled by COVID-19 and the increased need for digital services and easy access to COVID passes. In the first quarter of 2022, Italy reached the milestone of 30 million SPID accounts created – half the country's population – with10 million accounts activated in the last 12 months alone.[1] The SPID consists of a single set of credentials making it possible to enrol children at school, view health records, book a hospital visit or access tax records from a computer or smartphone. The system provides greater security than older style credentials and protects individuals against profiling – in which their data can

be accessed by third parties. The SPID is also used by private companies – for example, you can register with a bank using the digital SPID identity. It also, by default, conforms with eIDAS – the EU regulation on electronic identification and trust services – and grants access to public services provided by other EU member states that have joined the eIDAS node.[2]

In Belgium, the eID scheme, itsme, was delivered in 2017 by the private sector, with banks and telecom providers prominent, but still operates within a clear government-led regulatory framework. 70% of the adult population has adopted this eIDAS approved eID which allows easy and safe digital identity proofing and signing.[3] Adoption increased strongly after itsme was used as the authentication mechanism for the official CovidSafeBE app in 2021. The top digital government services that can be accessed with itsme are eHealth,

social security (MyPension, MyCareer, Student@Work, etc.) and online tax returns – followed by the My e-Box portal to locate all government documents and the digital service for the payment of unemployment benefits.[4]

In other countries the private sector has played an even bigger role in the success of eID schemes. For example, Norway's and Sweden's BankID schemes have achieved over 70% adoption within the adult population.[5] The schemes are run fully by commercial entities owned by local banks, with governments only setting out the guiding principles. BankID can be used for financial services such as loan applications and for government service access such as tax returns, healthcare services etc.

Switzerland's window of opportunity

By comparison, the development and uptake of eID schemes in Switzerland has been minimal. Only a few local administrations have introduced schemes in recent years. For example, the Schaffhausen eID+ now allows cantonal residents to set up an electronic identity on their smartphone to access various digital public services easily and securely without additional logins and passwords.[6] The Canton of Zug offers a blockchain-based eID, where citizens register through the online portal ZUGLOGIN and eZug app to access digital services of the public administration and administrative court. In addition, entries that previously had to be signed by hand can also be signed and submitted electronically via ZUGLOGIN.[7]

A few other cantons – such as Jura, Solothurn, Berne and Aargau – have adopted the private sector solution, SwissID of SwissSign, to gain access to public services.[8] However, the situation in Switzerland remains a cantonal patchwork of different eIDs with no clear or co-ordinated interoperability between the different systems.

The introduction of a national law related to the eID was rejected by a clear majority of Swiss voters in March 2021 – mainly because the government had planned to delegate the issuing of eIDs to the private sector. The findings of **The Deloitte Swiss Digital Government Study 2021** confirmed the public's reservations about involving both the public and private sector. 84% of respondents preferred the provision of eID services (for example, creating an electronic identity: notary online) by the state and not a private company.

However, this initial rejection of the proposed eID law presents a clear opportunity to develop a more viable future eID solution, based on best practices and international success stories. Opening the consultation for the adjusted eID law, the Federal Council has already highlighted the role of the state as the issuer and operator of the infrastructure, the focus on self-sovereign identities (SSI), the importance of data protection and the gradual opening up of the new infrastructure to the private sector.[9]
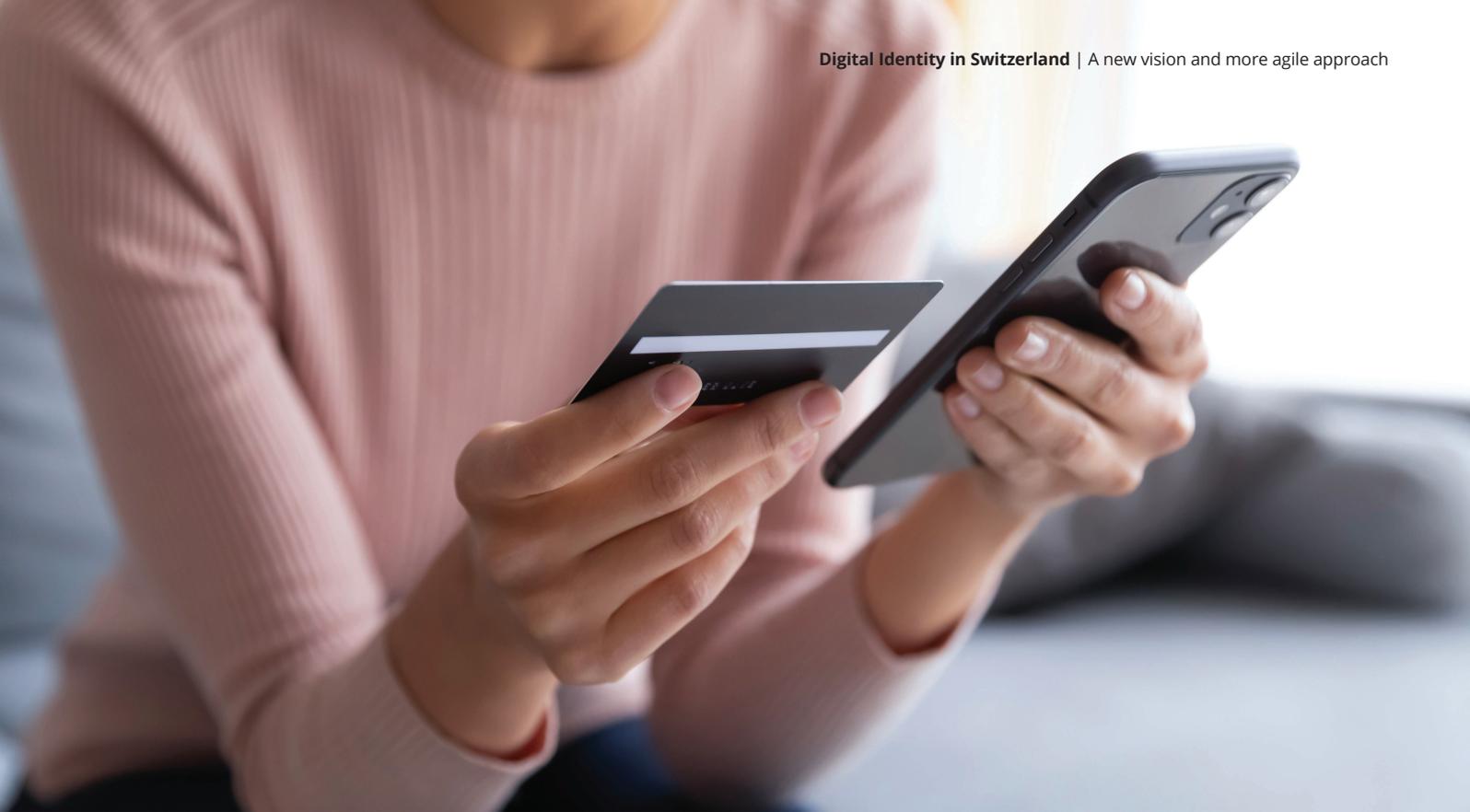
Key success factors for eID in Switzerland

The following key factors will be essential to build a successful digital identity and a broader digital ecosystem.

1.Build trust:
First and foremost, governments need to build trust for their eID systems if these are to be adopted at scale. A successful roadmap includes not only building confidence that the solution is reliable, but also that all the players involved and the integrity of the system can be relied on.

2.Focus on user-control / self-sovereign identities (SSI):
Modern eID systems should be governed by individual choice. Users should have full control over whom they want to share data with and who sees what kind of information. Unlike paper IDs or records, digital eID systems can, for example, verify age without exposing the date of birth or confirm qualification for government programmes that require income validation, without disclosing full pay data.

3.Take data privacy seriously:
According to **The Deloitte Swiss Digital Government Study 2021**, some Swiss citizens have concerns about data privacy and cybersecurity when using new digital services. By minimising the flow of personal data in a future eID system, privacy can be protected. In addition, a secure technology solution and decentralised data storage – for example with blockchain/ distributed ledger technology – will further ensure privacy.

4.Develop and comply with standards:
As part of building trust and accountability it will be key to define local standards for an eID system and regulate the role of trust service providers (TSPs). International standards (for example, eIDAS) should be taken into account so that national eIDs are recognised abroad.

5.Enable interoperability with broader digital ecosystem:
However, trust, user-control/privacy and good regulation will not on their own drive adoption of eID systems. Everyday usage of the system will lead to increased participation – but this can only be achieved by making eID systems very easy for the private sector to use. **For example, digital identification systems can be enablers for other solutions such as electronic signing – as explained in Deloitte's latest e-Signature Blog**. Successful eIDs manage not only to integrate municipal and cantonal administrations, but the private sector as well.

End notes

1. BiometricUpdate.com, Italian national digital ID scheme reaches 30 million users milestone, 9.5.2022 (https://www.biometricupdate.com/202205/italian-national-digital-id-scheme-reaches-30-million-users-milestone)
2. MEF, Italy demonstrates success in mass adoption of a digital identity scheme with SPID, 7.9.2021 (https://mobileecosystemforum.com/2021/09/07/italy-demonstrates-success-in-mass-adoption-of-a-digital-identity-scheme-with-spid/)
3. Finextra, The Future of Digital Identity 2022: Global schema for digital identity wallets, 16.5.2022 (https://www.finextra.com/the-long-read/410/the-future-of-digital-identity-2022-global-schema-for-digital-identity-wallets)
4. Itsme, Belgians made massive use of itsme® in 2020, especially to connect to eHealth services, 26.2.2021 (https://www.itsme-id.com/blog/itsme-3years-fas)
5. Oliver Wyman, Digital Trust. How banks can secure our digital identity, 2021 (https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2021/nov/Digital-Trust-Final.pdf)
6. Kanton Schaffhausen, Schaffhauser eID+ (https://sh.ch/CMS/Webseite/Kanton-Schaffhausen/Beh-rde/Services/Schaffhauser-eID--2077281-DE.html)
7. Kanton Zug, Vereinfachter Zugang zu digitalem Geschäftsverkehr mit Behörden, 26.3.2021 (https://www.zg.ch/behoerden/finanzdirektion/direktionssekretariat/aktuell/vereinfachter-zugang-zu-digitalem-geschaeftsverkehr-mit-behoerden)
8. SwissID, Kanton St. Gallen setzt als Login zum Bürgerkonto die SwissID ein, 16,12,2020 (https://www.swissid.ch/en/news/detail-page~newsID=e70482cf-ec8d-44a6-84d0-f0a79934ed67~.html)
9. Der Bundesrat, E-ID: Bundesrat eröffnet Vernehmlassung, Medienmitteilung, 29.6.2022 (https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-89515.html)

Contacts and authors

Rolf Brügger
Partner
Government & Public Services
rbruegger@deloitte.ch
+41 58 279 7714

Daniel Hirs
Director
Operational Model
Transformation Lead
dahirs@deloitte.ch
+41 58 279 7273

Deloitte.