www.pwc.ch

Digital identity

Your key to unlock the digital transformation

pwc

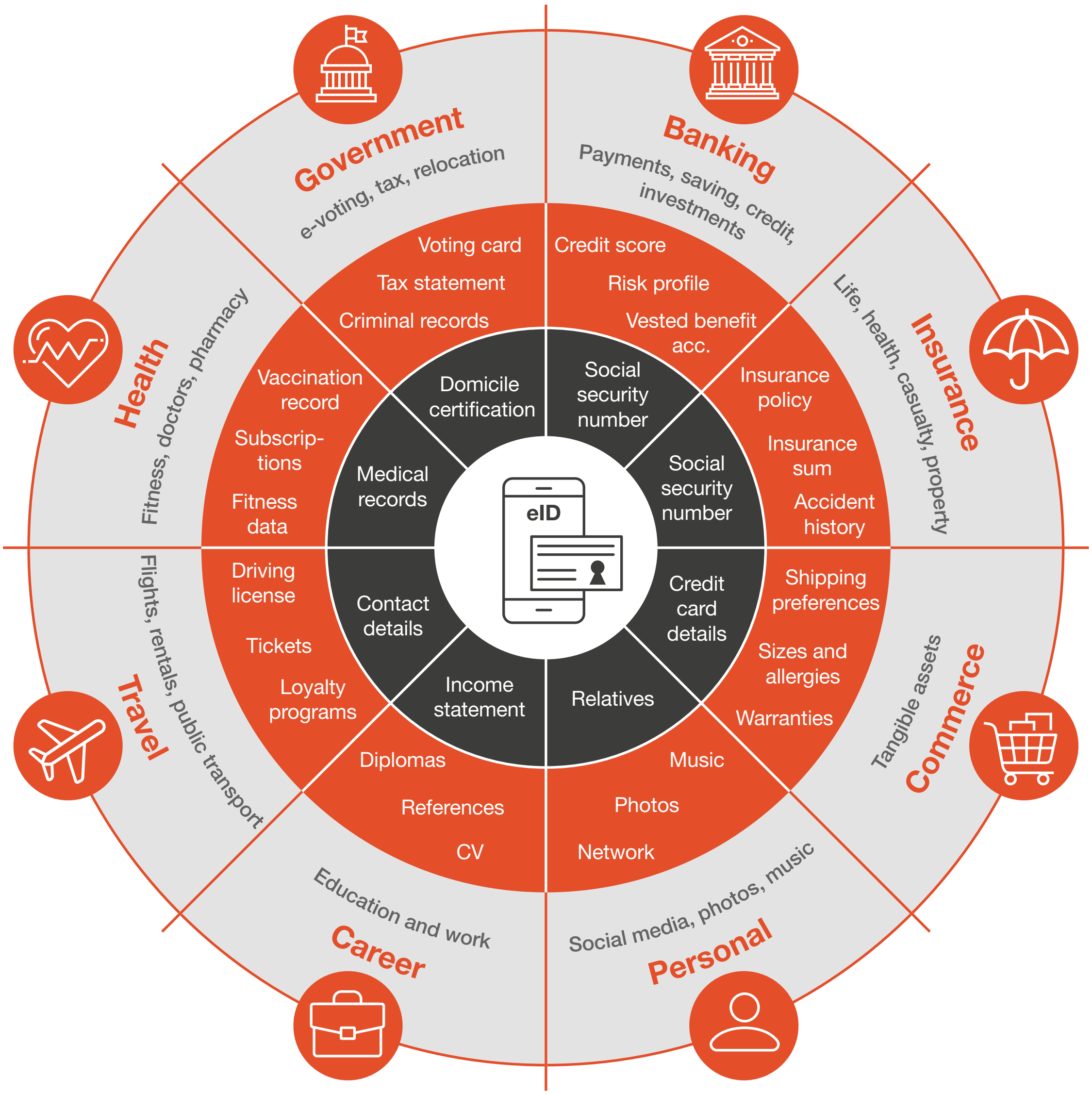
A universally usable digital identity represents an opportunity for companies to reduce risks and realise considerable cost savings by increasing process efficiency and de-facto outsourcing customer identification.

Contents

1 A growing need for a digital identity

Identity is a precondition for participating in society by facilitating access to health and welfare systems, education, and financial and government services. With the accelerating digital transformation, a rapidly growing number of transactions is conducted online, creating an ever-more-urgent need for a digital identity.

Based on verified personal information, a digital identity can be defined as a set of digitally captured and stored attributes such as name, date of birth or gender coupled with credentials that are linked to a unique identifier to identify a person and thereby facilitate transactions in the digital world. In the future, the core digital identity attributes may be complemented with additional attributes and documents from all areas of life such as social security number, medical records or school diplomas, catalysing the digital transformation for countless use-cases ranging from opening a bank account and taking out an insurance policy to filing a tax return.



eID Verified core identity: Name, first name, gender, nationality, place of birth, facial image, reg. nr.

□ Use-case area

■ General data

🟥 Industry-specific data

Before we were aware how extensively the internet would proliferate into our everyday lives, the internet was built without a native identity layer. In the absence of a standardised way to identify people or entities, every website started to create its own digital identity solution with its own local accounts and passwords. As a result, people collect in their digital interactions a multitude of digital identities ranging from different e-mail accounts and social media profiles to e-banking accounts.

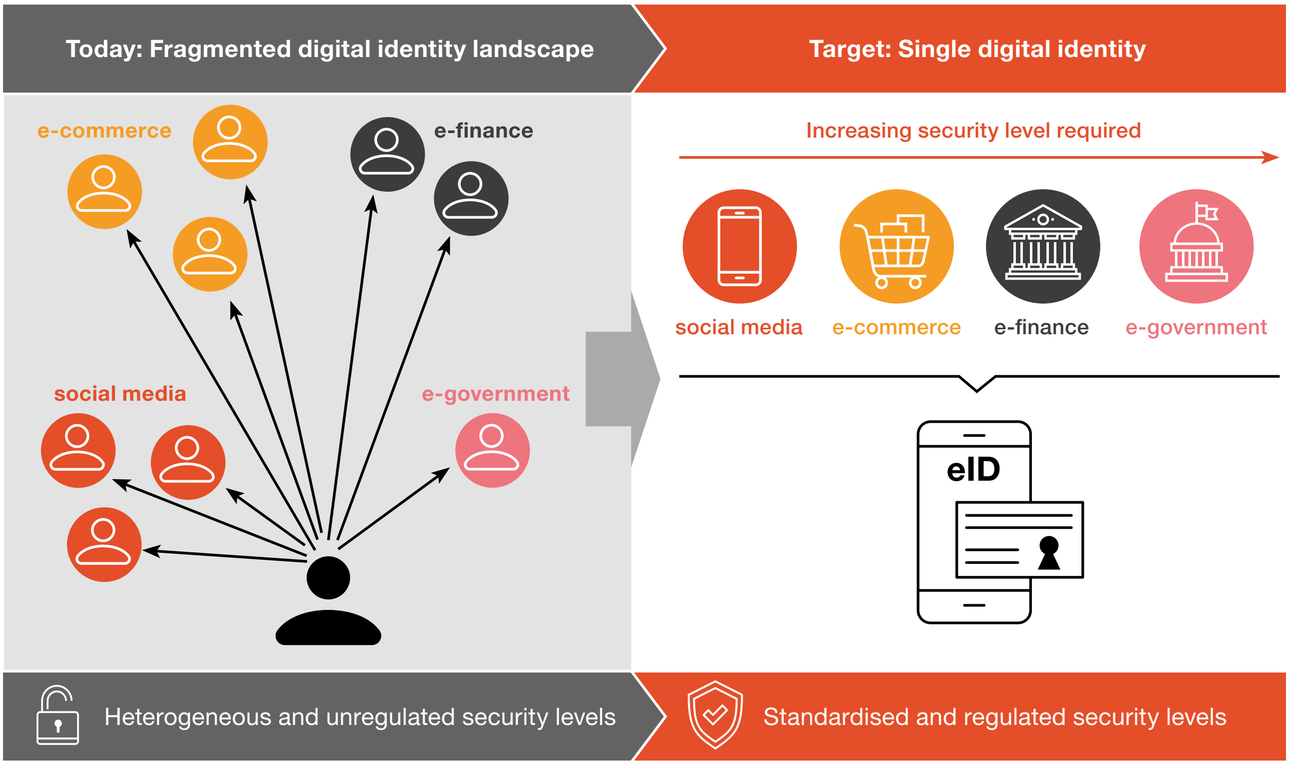
The ability to use the internet without revealing your real identity is not necessarily bad. When using certain digital services, like sharing content on social media, a pseudonym is more than sufficient. In some instances, such as exercising the right to freedom of expression in an authoritarian state, remaining anonymous is key. In many other cases, for example when opening a bank account or taking out an insurance policy, companies are required to know the identity of their counterparty by law.

Despite the positive aspects, it is clear that today's fragmented digital identity landscape, with its large number of accounts and passwords, comes at a cost. For users, having an unmanageable number of accounts and passwords is time-consuming and inconvenient, as they have to register their identity data repeatedly with every new counterparty and often lose access to their accounts. From a security perspective, today's fragmented digital identity landscape is unregulated and characterised by a daunting number of heterogeneous and unregulated security levels. Faced with this complexity, many users neglect security concerns and use the same simple password across many different services.

By contrast, a single digital identity has the potential to significantly improve both user experience and convenience by making a wide range of digital services accessible in a seamless fashion and rendering repeated registration obsolete. In addition, users will be able to regain control over their digital identity by being able to manage which attributes they want to share with which counterparty. At the same time, "putting all your eggs in one basket" and entrusting a single digital identity ecosystem with managing your digital identity leads to an elevated cluster risk in case of an attack, technical failure or malicious behaviour. Despite these security concerns, the overall security situation is expected to improve for the average user thanks to lower complexity as well as standardised and clearly regulated security levels across the entire digital identity ecosystem.

From a business point of view, the identification of the same customer is redundantly replicated with every company a customer has a business relationship with. This means every company has to develop and maintain their own costly and often largely paper-based identification processes for onboarding new clients as well as authenticating existing clients in order to provide services to them. In addition, every business has to periodically review and update the customer data to reflect any changes.

With this in mind, a universally usable digital identity represents an opportunity for companies to reduce risks and realise considerable cost savings by increasing process efficiency and de-facto outsourcing customer identification. Businesses can increase their conversion rates by lowering the threshold to conclude a transaction and by launching new products and services with a superior user experience to help them gain a competitive edge.


Today: Fragmented digital identity landscape
e-commerce
e-finance
social media
e-government
Heterogeneous and unregulated security levels
Target: Single digital identity
Increasing security level required
social media
e-commerce
e-finance
e-government
eID
Standardised and regulated security levels

2 Understanding digital identity

2.1 Digital identity ecosystem

The provision and usage of digital identity involves a number of interdependent actors, who collectively form a digital identity ecosystem. Confronted with increasing complexity due to growing transaction volumes and increasing customer expectations, any successfully digital identity ecosystem requires a collaborative effort across organisations and industries.

Across all stages of the digital identity lifecycle, every actor takes on certain tasks or operations that are associated with their role. But digital identity systems can come in many different forms. The number of defined roles and the scope of their activities largely depend on the specific requirements of a country's legal framework and the players involved.

Hence, a set of archetypical roles in a digital identity ecosystem will be introduced. The first three core roles Identity Owner, Identity Provider and Relying Party represent the minimum for any digital identity ecosystem and are also covered in Switzerland's emerging regulatory framework (see section 4). The three roles Broker, Attribute Provider and Service Provider are labelled as ecosystem-dependent roles as they can be incorporated in a digital identity ecosystem as needed. It is important to note that these generic roles can be further subdivided to accommodate different circumstances and requirements.

In practice, the key question when designing a digital identity ecosystem is whether to adopt a model that is broker centric or Identity Provider centric.

Identity Owner (IO)	• Owner and controller of a digital identity • Uses their digital identity to conveniently and securely identify themselves in digital transactions • Natural person (e.g. Alice or Bob)
Identity provider (IdP)	• Responsible for the provision of a digital identity • Verifies an individual's identity and issues the corresponding digital credentials to ascertain their digital identity • Government agency (e.g. passport office) or government-recognised organisation (e.g. bank)
Relying Party (RP)	• Relies on a digital identity for onboarding of new customers and authentication of existing customers • Integrates digital identity in its operating model to improve the user experience and increase efficiency • Industry-agnostic role including businesses (e.g. online shops) and government agencies (e.g. tax offices)
Broker	• Ensures interoperability in the ecosystem and enhances privacy by preventing tracking actions across different roles • Intermediates the data flow between the Identity Provider and the Relying Party • Neutral organisation (e.g. infrastructure provider)
Attribute Provider (AP)	• Offers additional attributes that are not collected by the Identity Provider during registration • Additional attributes allow Relying Parties to accelerate their digital processes and offer more tailored services • Government agency (e.g. fedpol), state-affiliated company (e.g. Post) or private company (e.g. Telco)
Service provider	• Offers electronic trust services such as digital signatures • Electronic trust services allow providers to enhance and expand the interactions and services within the ecosystem • Private company (e.g. Telco)

🟥 Core roles 🟧 Ecosystem-dependent roles

Identity Provider centric

In an Identity Provider-centric model, the data flows directly from the Identity Provider to the Relying Party, and vice-versa. Hence, the actions of the Identity Owner can be traced across the ecosystem. For example, the Identity Provider could track how often the Identity Owner logs into an online casino, while the casino might register which institution the Identity Owner has registered their digital identity with.

Broker centric

In a broker-centric model, an identity broker intermediates the data flow between the Identity Provider and the Relying Party to ensure interoperability and enhance the system's overall privacy by "blinding" the Identity Provider and Relying Party from one another. This means the Identity Owner's actions cannot be traced.

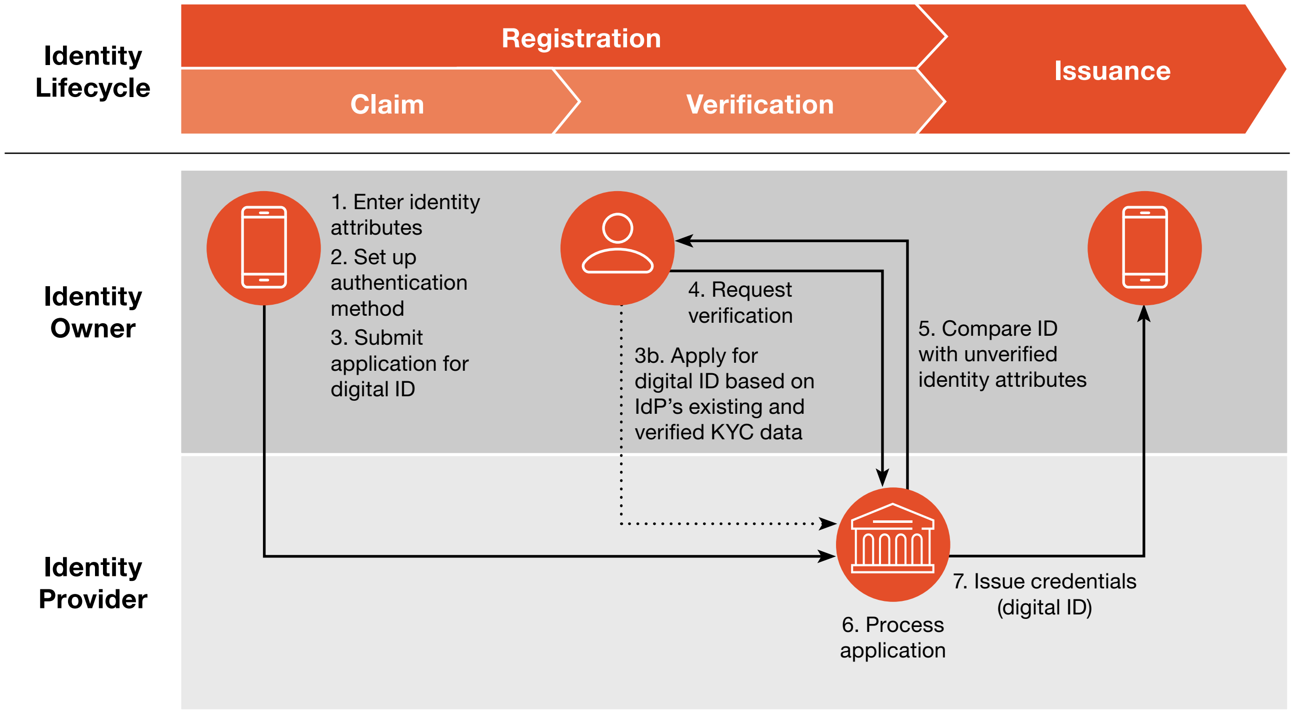
However, channelling the entire data flow through the broker as a central authority introduces a single point of failure and creates a honeypot with a vast quantity of valuable data. Implementing a broker based on a private blockchain like in the case of the Canadian digital identity solution (developed by SecureKey) could offer a solution to this issue and meet the so-called triple-blindness requirement.

2.2 Digital identity lifecycle model

The provision and usage of digital identity is not a single, one-time event, but rather a sequence of (recurring) events, which can be conceptualised in a lifecycle model. In the following, a generic end-to-end digital identity lifecycle will be introduced based on a broker-centric digital identity ecosystem.

Registration

The registration stage initiates the digital identity lifecycle and can be further subdivided into claiming and verifying digital identity. (1) In a first step, the Identity Owner registers their digital identity by entering a set of required identity attributes in the Identity Provider's web or mobile application. The attributes can be categorised as biographical data such as name, gender, address, biometrical information (e.g. fingerprint, iris scan) and / or additional data formats such as behavioural data. (2) Depending on the chosen security level, the Identity Owner has to set up an appropriate authentication method. In the case of 2 Factor Authentication (2FA), this includes a first as well as a second factor of their choice. (3) The completed application is then submitted to the Identity Provider.


Identity Lifecycle
Registration
Claim
Verification
Issuance
Identity Owner
Identity Provider
1. Enter identity attributes
2. Set up authentication method
3. Submit application for digital ID
4. Request verification
3b. Apply for digital ID based on IdP's existing and verified KYC data
5. Compare ID with unverified identity attributes
6. Process application
7. Issue credentials (digital ID)

Verification

In a next step, (4) the Identity Owner requests verification of their identity data. In response, (5) the Identity Provider verifies the claimed identity against existing data. This is necessary to ascertain whether the claimed identity exists and is unique (deduplication). In most cases, the verification is based on at least one official government ID. Depending on the desired security level, this step is executed as face-to-face verification at the Identity Provider's premises or through an equivalent online presence such as a video identification (see also FINMA Circular 2016/7 Video and online identification).

Depending on the design of the digital identity ecosystem, (3b) the Identity Owner can shorten the registration process and leverage an existing business relationship. Identity Providers (i.e. banks) can reuse the verified identity data they have already collected to meet their Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) obligations.

Issuance

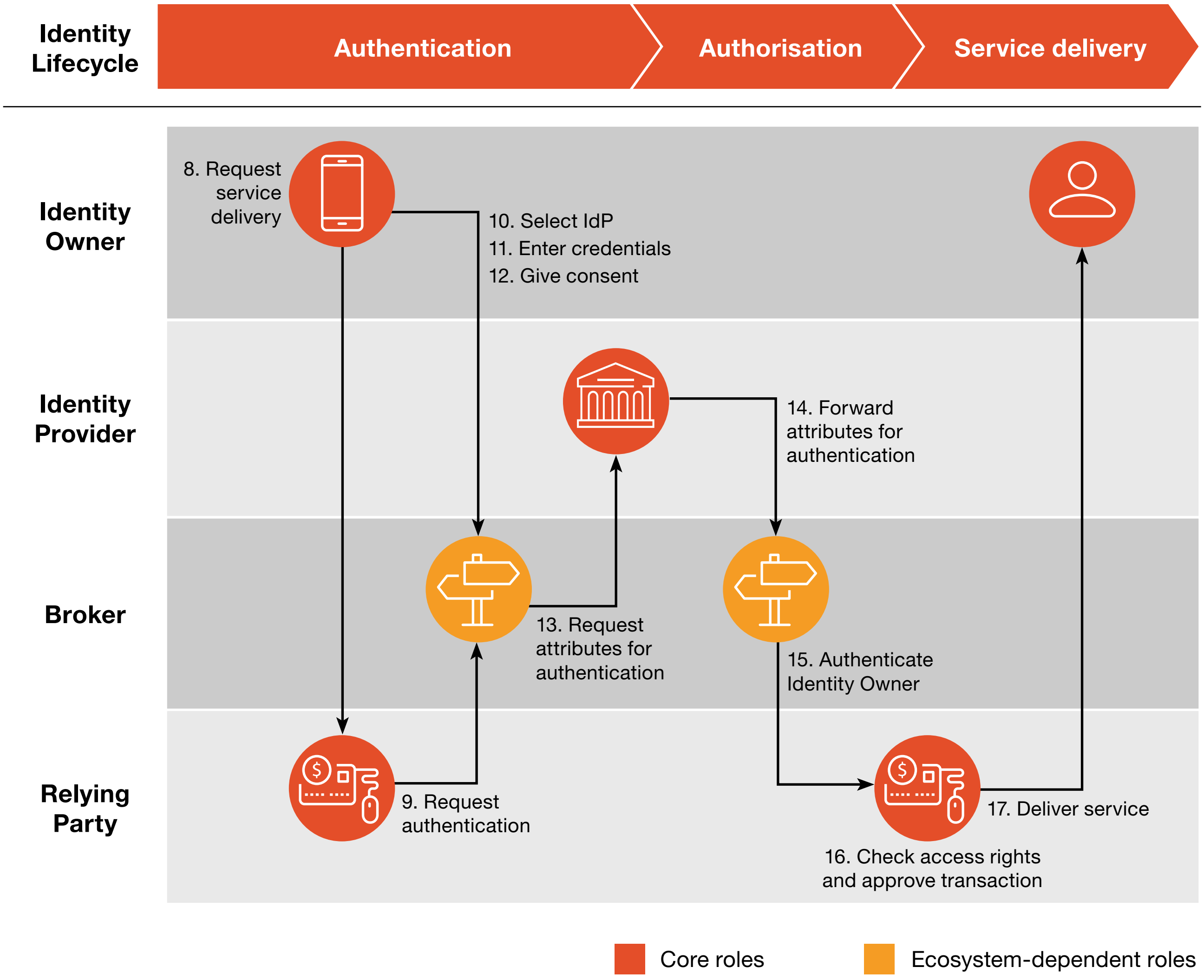
Once the Identity Owner's identity is successfully verified, (6) the Identity Provider processes the Identity Owner's application and (7) issues the credentials in the form of a digital identity. With the issuance of credentials, the Identity Provider ascertains the Identity Owner's identity by authoritatively linking the digital identity via a unique identifier to at least one authenticator. Credentials can be categorised as something you know (e.g. password or PIN), something you are (e.g. biometrical information such as a fingerprint) or something you have (e.g. ID card or security token).

Authentication

(8) The Identity Owner can now use their digital identity to access and request digital services, such as signing into the web portal of an airline to purchase a flight ticket. (9) In order to provide the required service, the Relying Party needs to authenticate the requestor. In a broker-centric digital identity ecosystem, the Identity Owner is redirected for the purpose of authentication to the broker's mobile or web portal. At this point, the Identity Owner is asked to (10) select their preferred Identity Provider for this transaction, (11) present one or more (digital) credentials to prove their identity and (12) give consent to share the requested identity attributes with the Relying Party on a one-time or time-bound basis. As soon as the authentication request is fully approved by the Identity Owner, (13) the broker requests the desired identity attributes from the chosen Identity Provider and (14) transmits the received data to the requesting Relying Party for authentication of the Identity Owner.

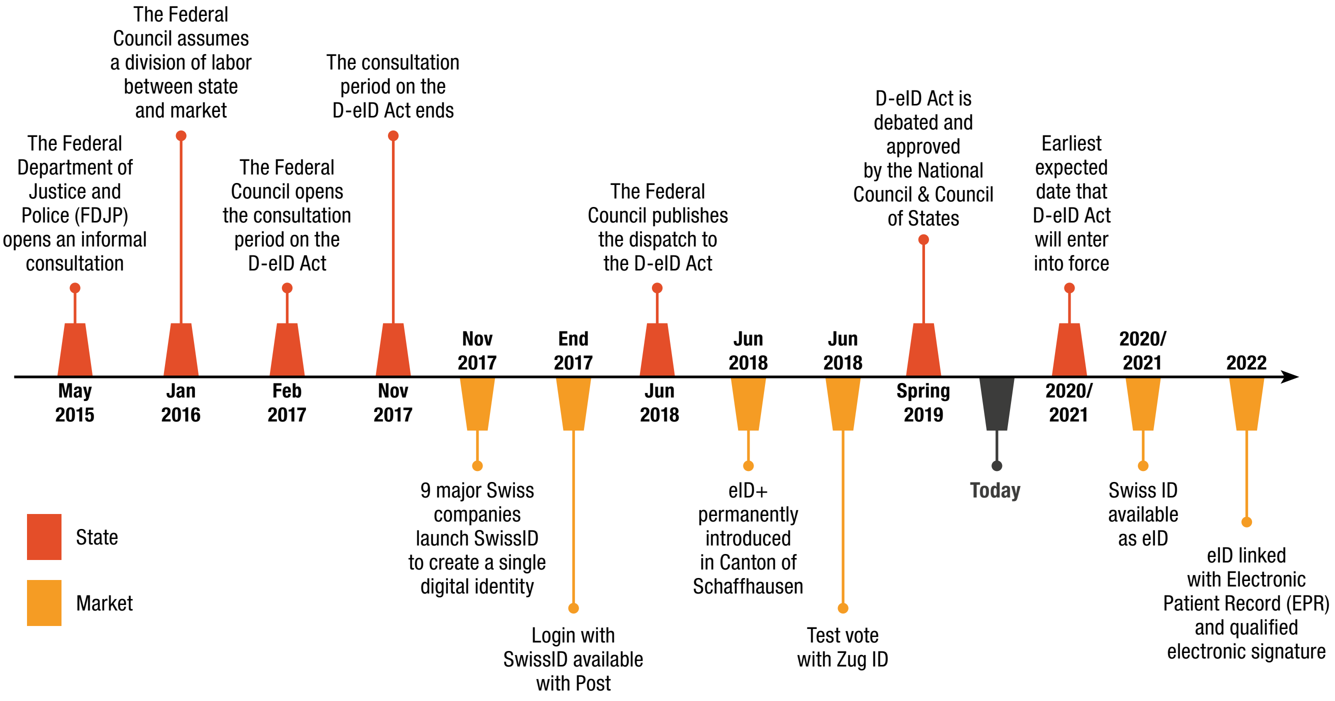
Authorisation and service delivery

(15) After having authenticated the requestor, (16) the Relying Party checks as part of the authorisation process which rights are associated with the user's digital identity. If the result of the authorisation is positive, the transaction can be approved and (17) the requested service is delivered to the Identity Owner.



Identity Lifecycle
Authentication
Authorisation
Service delivery
Identity Owner
Identity Provider
Broker
Relying Party
8. Request service delivery
10. Select IdP
11. Enter credentials
12. Give consent
14. Forward attributes for authentication
13. Request attributes for authentication
15. Authenticate Identity Owner
9. Request authentication
17. Deliver service
16. Check access rights and approve transaction
Core roles
Ecosystem-dependent roles

3 Digital identity in Switzerland: Where do we stand today?



May 2015
The Federal Department of Justice and Police (FDJP) opens an informal consultation
Jan 2016
The Federal Council assumes a division of labor between state and market
Feb 2017
The Federal Council opens the consultation period on the D-eID Act
Nov 2017
The consultation period on the D-eID Act ends
Nov 2017
9 major Swiss companies launch SwissID to create a single digital identity
End 2017
Login with SwissID available with Post
Jun 2018
The Federal Council publishes the dispatch to the D-eID Act
Jun 2018
eID+ permanently introduced in Canton of Schaffhausen
Jun 2018
Test vote with Zug ID
Spring 2019
D-eID Act is debated and approved by the National Council & Council of States
Today
2020/ 2021
Earliest expected date that D-eID Act will enter into force
2020/ 2021
Swiss ID available as eID
2022
eID linked with Electronic Patient Record (EPR) and qualified electronic signature
State
Market

Acknowledging the need for a digital identity, the Federal Department of Police started working on a concept for an electronic Identification Document (eID) in 2013. Mirroring the physical world, this initial approach assumed the issuance of an electronic or digital identity to be solely a state responsibility. In 2015, the Federal Department of Justice and Police (FDJP) initiated a broad stakeholder consultation involving cantons, industry associations and major companies. The results as well as insights from similar initiatives in other countries suggested that state-developed digital identity solutions lead to comparatively higher IT costs and are not flexible enough to adapt to rapidly changing market needs and technological advancements.

Based on these findings, the Federal Council announced in early 2016 a division of tasks and responsibilities between state and market: market actors will develop and run digital identity systems based on the latest technology, while the government will provide the corresponding regulatory framework, certify private Identity Providers and provide verified identification data including a unique identifier.

The consultation period on the Draft Federal Act on Electronic Identification Services (D-eID Act) took place between February 2017 and November 2017. The role of the state remained a highly controversial topic among the 62 respondents as many of them rejected the idea of the private sector being in charge of issuing digital identity. Not surprisingly, ensuring the highest level of security and privacy was a priority for all stakeholders.

At the Swiss Digital Day in November 2017, a consortium of nine major Swiss companies announced the launch of the initiative SwissID to develop a single digital identity for the Swiss market. Adopting a gradual approach, SwissID aims to create an entire ecosystem offering a suite of different identity services ranging from authentication to electronic signature.

Shortly after this, the Swiss Post started migrating all their user accounts to a SwissID solution with basic login functionality. Despite receiving mixed reactions from Post customers, the SwissID consortium was able to establish a substantial user base right from the start. In March 2018, SwissSign Group AG was founded to advance the development of SwissID. Today, the basic SwissID can also be used as a single login with other companies like Blick, Bilanz, St. Galler Kantonalbank or the Canton of Graubünden. SBB, the Canton of Zug, Mobiliar and AXA Wintherthur are expected to follow soon, among others.

In early summer 2018, two other Swiss digital identity solutions made a name for themselves. Following a four-month pilot phase, the Canton of Schaffhausen permanently introduced its own digital identity solution in the shape of eID+.

Developed in cooperation with the Zurich-based start-up Procivis, eID+ allows its users to access a growing number of e-government services. In April 2019, Procivis announced a partnership with the electronic signature provider Skribble to combine digital identity with legally binding electronic signatures.

Living up to its reputation as Crypto Valley, in November 2017 the city of Zug started running a pilot with the world's first blockchain-based digital identity. Leveraging uPort's technology stack, the IT company ti&m implemented the ZugID as a so-called self-sovereign identity. Being independent of any form of centralised control, the concept of self-sovereign identity aims to grant the user full autonomy and control over their identity. In June 2018, the ZugID was successfully used for a non-binding referendum.

In the 2019 spring session, the National Council endorsed the Draft Federal Act on Electronic Identification Services (D-eID Act) (see section 4 for more details), and thus took an important step towards a state-recognised electronic identity. In the 2019 summer session, the Council of States followed suit and passed the bill.

In view of the steadily increasing number of transactions processed digitally, the need for an electronic identity itself was largely undisputed in both chambers. However, the regulation's basic thrust of assuming a division of roles between the state and the private sector was a point of contention in the debate in the Swiss parliament. Many politicians consider the issuance of physical as well as digital means of identification to be an exclusive task of the Swiss Confederation. Despite these concerns, the new legislation intends to combine the confidence-building effect of state recognition and private-sector dynamism to facilitate a secure and user-friendly solution and thus ensure the success of the eID. The bill is not expected to enter into force until 2020/2021 at the earliest, unless a referendum is held.

These recent developments in the market – but also from the government – indicate that digital identity is gaining momentum in Switzerland. Hence, it is not so much a question of whether a digital identity solution will be introduced on the national scale, but rather when it will be introduced and what a successful model will look like.

4 Draft Federal Act on Electronic Identification Services (D-eID Act)

The Draft Federal Act on Electronic Identification Services (D-eID Act) creates the legal basis for a state-recognised electronic identity in Switzerland and enables natural persons to identify themselves securely and easily in electronic business transactions with companies and authorities. The bill regulates the entire lifecycle of electronic means of identification from issuance to revocation and defines the rights and obligations of the various actors in the ecosystem of an electronic identity. The following figure illustrates the key pillars of the D-eID Act and elaborates on the associated regulatory provisions.

4.1 Roles and responsibilities

In section 2.1, a set of archetypical roles in a generic digital identity ecosystem were introduced. In the case of Switzerland's emerging digital identity ecosystem, the Draft Federal Act on Electronic Identification Services clearly defines and regulates the relevant ecosystem roles and the associated rights and responsibilities.

Swiss citizens and foreigners with a valid ID as specified in the Federal Act on Foreign Nationals and Integration (FNIA), or foreigners whose identity can be proved in a special procedure, are eligible for an eID and can act as Identity Owner. The eID is personal, non-transferrable and voluntary. The owner of an eID has to exercise a duty of care to prevent abuse of their eID.

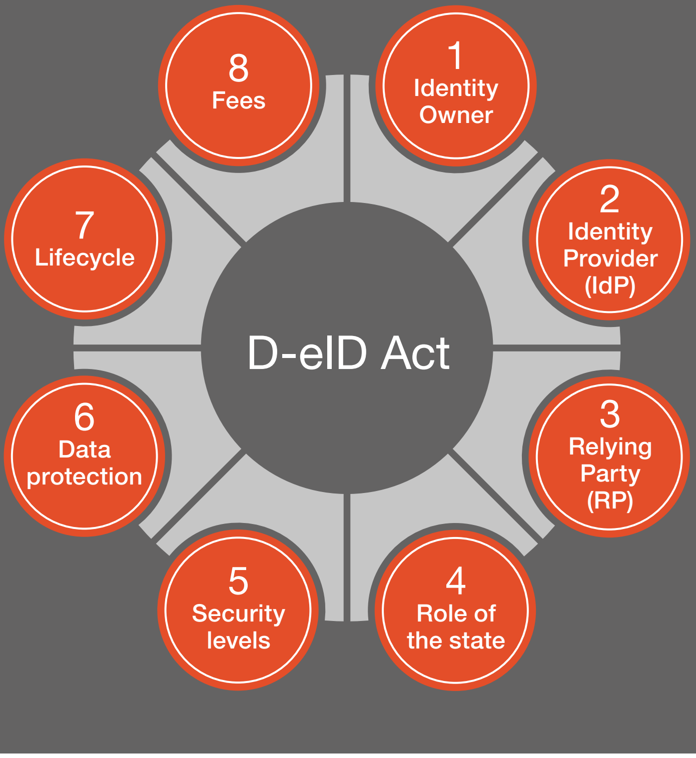
While issuing an ID is traditionally a sovereign task of state authorities, the Draft Federal Act on Electronic Identification Services (D-eID Act) assumes collaboration between the state and the private sector to provide digital identity. In this process, the trust-building effect of state recognition is combined with the market's flexibility and technological expertise to ensure the rapid proliferation of the eID in Switzerland.

Hence, private companies have been entrusted with the provision of digital or electronic identity (eID). To issue an eID, Identity Providers are required to obtain formal recognition from the newly created federal eID Commission (EIDCOM). Recognition is granted for three years and requires compliance with a number of (operational) requirements such as, for example, entry in the commercial registry, skilled staff, compliance with the security requirements for the eID systems, or reporting to the authorities.

Despite the aforementioned division of responsibility, the state still plays a pivotal role in the digital identity ecosystem. With EIDCOM, an independent federal organisation will be created to monitor compliance with the Draft Federal Act on Electronic Identification Services and to take the necessary decisions to ensure a smooth-functioning eID ecosystem. Among other tasks, EIDCOM is responsible for recognising Identity Providers and publishing a list containing all recognised Identity Providers, as well as maintaining an information system to support their activities.

The Federal Office of Police (fedpol) is responsible for verifying the applicant's identity and providing verified personal identification data to the Identity Provider, as well as maintaining an information system to support fedpol's activities.

Relying Parties need a contractual agreement with the Identity Provider defining the desired security level as well as organisational and technical processes in order to be able to use the eID as a means of identification. Aiming at interoperability within the ecosystem, the eID Act obliges Relying Parties to accept any eID for the required security level. The eID registration number, which is issued by fedpol, can be used for identification purposes.



1 Identity Owner	• Requirements for applying for an eID: (Art. 3) a. Swiss citizens with valid ID b. Foreigners with valid ID based on FNIA c. Foreigners whose identity can be proved in a special procedure	• The eID is personal, non-transferrable (Art. 12) and voluntary (Art. 3) • A duty of care applies to the owner to prevent abuse (Art. 12)
2 Identity Provider (IdP)	• Issuing eIDs requires formal recognition from eID-Commission (EIDCOM) (Art. 13) • Identity Providers ensure interoperability of their eID solutions	• Recognition is granted for three years (Art. 14) and requires meeting (operational) requirements such as such as skilled staff, data protection & security and reporting (Art. 15)
3 Relying Party (RP)	• Relying Parties need a contractual agreement with the Identity Provider to define security level as well as organisational and technical processes (Art. 20)	• Relying Parties can use the eID registration number for identification (Art 21) • Relying Parties are required to accept any eID for the required security level (Art. 22)
4 Role of the state	Like in the physical world, the state assumes a pivotal role in the digital identity ecosystem: • The federal office police (fedpol) is responsible for identity verification, providing verified personal identification data to the Identity provider (Art. 6) and assigning the Identity Owner a unique eID registration number	• The EIDCOM is responsible for the IdP recognition and publishing a list with all IdPs (Art. 25) as well as maintaining an information system to support their activities (Art .24)
5 Security levels	• 3 different security levels: Low, Substantial, High (Art.4) • Principal of downward compatibility (Art. 4): An eID issued with a higher security level can also be used, if a lower level is required	• The security levels differ by the number of personal identification attributes (Art. 5) as well as the rules for issuance, usage and operation (Art. 6)
6 Data protection	In some aspects, the data protection provisions of the eID Act go beyond the Federal Act on Data Protection: • Processing of personal identification data is limited to the purpose of identification as long as the eID is valid (Art. 9)	• The transfer of personal identification data is limited to the necessary minimum and requires consent (Art. 16) • Personal Identification data, usage data and other data have to be kept segregated (Art. 9)
7 Lifecycle	• An eID is issued by the Identity Provider together with an authentication mean after the fedpol has verified the applicant's identity and assigned him an eID registration number (Art. 6)	• An eID can be temporarily blocked by the IdP for example in the event of suspected fraud or loss of the password • The fedpol can revoke the eID registration number, if the eID is no longer used on a permanent basis
8 Fees	• The fedpol and the EIDCOM can charge fees on a pay-per-use basis for their provisions and services. The Federal Council specifies the fees in an ordinance and considers whether an IdP charges a fee for issuing an eID. (Art. 27)	• Queries regarding the validity of an eID are free of charge (Art. 27)

Analysis based on the version adopted by the Council of States

Security level	Goal	Attributes	Registration	Authentication	Attribute update frequency
Low	**Reduced threat of identity fraud and identity modification**	• eID registration no. • Official last name • Official first name • Date of birth	Online, based on official ID	1 Factor authentication (1FA) (e.g. password)	1 x year
Sub-stantial	**High protection against the threat of identity fraud and identity modification**	• Gender • Place of birth • Nationality	Personal or equivalent virtual presence at IdP based on official ID	2 Factor authentication (2FA) (e.g. password + SMS)	1 x quarter
High	**Highest protection against the threat of identity fraud and identity modification**	• Facial image (from fedpol database)	Personal or equivalent virtual presence at IdP based on official ID and additional docs	2 Factor authentication (2FA), at least 1 biometric (e.g. smartphone finger-print + SMS)	1 x week

4.2 Security levels and data protection

Security is a key concern when it comes to electronic identity. The Draft Federal Act on Electronic Identification Services (D-eID Act) differentiates between three security levels for the eID, as not all business processes have identical security requirements. In practice, overly strict security measures can be perceived as cumbersome and impede the mass-adoption of digital identity. As illustrated above, the security levels mainly differ in terms of the number of personal identification attributes, the attribute update frequency and the rules for registration and authentication, as well as the scope of application.

The security level low contains only basic attributes and is sufficient for online shopping (including age verification) or logging into a citizen portal. With more attributes and higher security standards for registration and authentication, the security level substantial is suitable for taking out an insurance policy online or opening a bank account online. Designed for the highest protection against the threat of identity fraud and identity modification, the security level high can be used for the most sensitive services like e-voting.

When an electronic identity is issued and used, sensitive and personal data is processed. Data protection and data security therefore enjoy the highest priority in the Swiss parliament. This is also reflected in the Federal Council's draft. In certain areas, the Draft Federal Act on Electronic Identification Services goes beyond the current level of protection of the Swiss Data Protection Act. For example, the Identity Provider may only pass on personal identification data to Relying Parties (e.g. online shops) for which the Identity Owner has consented. The Identity Provider must delete protocol data resulting from usage of the eID after six months. In addition, personal identification data, usage data and other data must be kept segregated. The Swiss Data Protection Act is also currently undergoing a total revision, and this could have important implications for the eID when it comes into force.

4.3 Lifecycle and fees

The eID Act regulates important steps of the digital identity lifecycle such as registration, blocking or revocation of the eID. In order to obtain an eID, the Identity Owner first has to apply for an eID with the Identity Provider. After an initial screening, the application is transmitted to fedpol for verification of the identity based on identity data in existing government registries. Subject to successful verification and the user's consent, fedpol transfers the applicant's personal identification data and the assigned eID registration number to the Identity Provider. By issuing a means of authentication to the Identity Provider, the Identity Provider activates the eID for use. In the event of suspected fraud or loss of the password, the Identity Provider can temporarily block an eID. If an eID is no longer used, fedpol can revoke the eID registration number permanently.

Fedpol as well as EIDCOM can charge fees for their services based on a pay-per-use model to finance their expenses. The Federal Council will specify the detailed fee model in an ordinance and take into account whether the Identity Providers provide their services free of charge. The fees for initial transfer of personal identification data during the issuance process can be waived to accelerate market adoption. For any further transfer, a fee in the double-digit centime range will be charged. Queries to check the validity of an eID are free of charge.

5 Main challenges for digital identity in Switzerland

5.1 A user perspective: Building trust in digital identity

Challenge

Building the user's trust in digital identity and its ecosystem is essential for the adoption of such an innovative technology, given the perceived security and privacy risks when entrusting a single digital identity ecosystem with the management of personal identity data and "putting all eggs in one basket."

Trust plays an essential role in the adoption process of digital identity, as experience with recent examples like e-commerce, e-banking and mobile banking shows. In the face of an increasing number of cyber threats ranging from data breaches and fraud to identity theft, users' concerns regarding the security and privacy of their identity data are among the primary barriers to the adoption of e-commerce and digital identity alike.

In the absence of existing knowledge or experience regarding digital identity, trust is a prerequisite to reduce the perceived security and privacy risks associated with the usage of such a new technology. If all actions could be executed with total certainty and there were no (perceived) risks, no trust would be needed. Providing the user with the necessary guarantees that their identity data will be protected is of paramount importance to gain and maintain the user's trust. With only a single incident, the user's trust might be irrevocably lost.

In today's fragmented digital identity landscape, the Identity Owner has to manage a multitude of unregulated digital identities issued by different organisations. Despite heterogeneous and largely non-transparent security levels, the Identity Owner has to trust all these organisations with the protection of their identity data in order to transact online.

When adopting a government-recognised digital identity like Swiss eID, the Identity Owner only has to trust a single digital identity ecosystem. Despite an elevated cluster risk, relying on a single Identity Provider will be more secure for the average user as the currently heterogeneous and unregulated security levels would be standardised across the ecosystem, helping to increase the overall security for the Identity Owner.

Besides the individual user's tendency to trust, structural assurances such as a strong regulatory framework (see section 4) or a best-in-class security and privacy framework are important determinants to build trust in a digital identity ecosystem. Building trust, however, is time-consuming and costly as it is based on long-term relationships and cumulative experience that provide the user with a sense of familiarity. Therefore, state agencies, state-affiliated companies as well as certain private actors such as banks or insurance companies benefit from their track record of handling sensitive data and are ideally positioned to leverage their reputation to instil trust in the digital identity ecosystem.

5.2 A business perspective: Succeeding in a two-sided market

Challenge

Digital identity systems represent a de facto, two-sided market with the Identity Provider as market operator. Like in any two-sided market, the success of a digital identity system heavily depends on the level of adoption among its two main customer groups. Hence, digital identity ecosystems face the challenge of the age-old “chicken-and-egg problem” – or which group do you get first, and how?

For both customer groups in a two-sided digital identity market – Identity Owners as well as Relying Parties – the utility of a digital identity system is a function of the number of participants on the other market side allowing them to realise positive network effects. In other words, Identity Owners are only willing to register for a digital identity if they can use it universally. For Relying Parties, integrating a digital identity solution into their systems and processes only pays off if they can reach a high number of customers and prospects. This means that strategies to solve the chicken-and-egg problem in Switzerland’s emerging digital identity ecosystem should be directed at both Identity Owners and Relying Parties.

Monetary subsidies are an effective measure to increase the level of adoption. Subsidising one side of the identity system raises the number of participants on the subsidised side, which makes the identity system more attractive for the other side. The Identity Provider can offset the costs of the subsidies in one market by higher demand and profit on the other side of the market. But who to subsidise? The optimal pricing strategy in a two-sided market is still being debated among economists. In principle, the less price-sensitive actor group should be charged a higher price to the benefit of the more price-sensitive market side. The challenge lies in reliably determining the price elasticity of the different actor groups and their willingness to pay.

However, findings from the rather unsuccessful digital identity project SuisseID permit preliminary inferences about how to design a more effective pricing strategy for a Swiss digital identity solution. In the case of SuisseID, the traditional pricing logic was applied to a two-sided market without considering the interdependencies between Identity Owners and Relying Parties. After an initial phase with state subsidies, Identity Owners had to pay a registration fee as well as an annual user fee. The registration costs made the ecosystem unattractive for new users, while the majority of existing users were not willing to renew their subscription.

Hence, a successful digital identity ecosystem in Switzerland should provide free digital identities to Identity Owners and base the business case on fees from the Relying Parties and additional services. Especially in the ecosystem’s early stages, monetary incentives for Relying Parties in the form of discounts are also advisable to create momentum.

Another effective strategy to overcome the “chicken-and-egg problem” is to attract high-value users first. In the case of digital identity systems, onboarding high-value Relying Parties such as large banks, telecommunication or e-commerce companies can significantly increase a digital identity’s overall attractiveness for Identity Owners, as they can use it more broadly. Once the Identity Owner is accustomed to using their digital identity when interacting with these high-value Relying Parties, they expect the same level of convenience from other companies too, which creates competitive pressure for other Relying Parties to follow suit.

While adopting eID yields many benefits for Relying Parties, it is vital to smooth their transition into Switzerland’s emerging digital identity ecosystem by lowering the technical and operational entry barriers. This is particularly important in the case of small or mid-sized public or private organisations lacking the capabilities and/or resources for a large-scale digital identity implementation project. The onboarding of Relying Parties should follow a streamlined process and leverage an existing contractual framework. From a technical perspective, a broker intermediating Relying Parties and Identity Providers can ease technical integration in times of scarce IT resources. Instead of being required to build interfaces to multiple Identity Providers, the broker serves as the single point of contact for the Relying Party.

One of the most effective strategies to overcome the chicken-and-egg problem is to tap into an existing pool of users. Today, most Identity Owners already have (multiple) digital identities that could potentially be leveraged to minimise the effort to obtain an eID.

The Draft Federal Act on Electronic Identification Services provides for a mechanism to transfer existing electronic means of identification to a recognised eID during a two-year transition period. The security level of the transferred eID is determined by the security requirements of the underlying customer identification process.

Banks in particular are ideally positioned to leverage their existing e-banking solutions and transfer them to a recognised eID with the security level substantial, as they are based on a strict verification process as required by Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) regulations. If the Bank ID does not meet the requirements of the security level substantial, additional measures have to be taken to perform a so-called step-up to the higher security level.

Once the Identity Owner trusts in the digital identity ecosystem and has embarked on their personal digital identity journey, it is essential to provide them with a seamless user experience throughout the entire digital identity lifecycle from registration to authentication.

When adopting a user-centric design perspective, it is essential to focus on the user's needs and reduce the effort involved in registering and using a digital identity to an absolute minimum. For the user, digital identity is a means to an end that allows them to simplify access to desired digital services. In this sense, a successful digital identity system should be accessible for the average user and not require an advanced skillset.

5.3 A regulatory perspective: Dealing with legal uncertainty and regulatory complexity

Challenge

Organisations intending to incorporate digital identity in their operating model are currently still confronted with a high degree of legal uncertainty, as the Draft Federal Act on Electronic Identification Services (D-eID Act) remains subject to change. As digital identity is expected to span many areas of life, a multitude of other European and national standards have to be considered when implementing or participating in a digital identity ecosystem.

In spring 2019, the Draft Federal Act on Electronic Identification Services (D-eID Act) was adopted by the National Council and the Council of States. Given the controversy regarding the role of the state in a digital identity ecosystem, companies are advised also to consider alternative scenarios during their initial assessment.

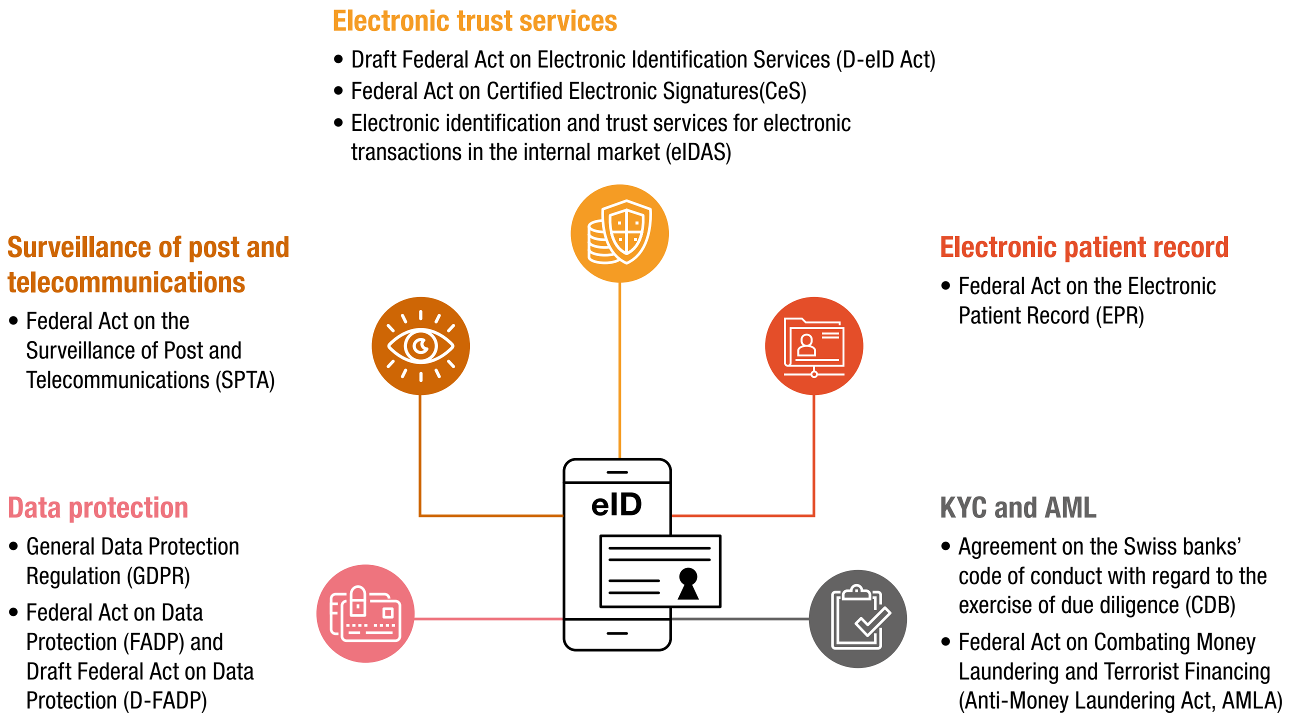
Looking at the current draft legislation, it becomes evident that the D-eID Act contains an unusually high number of delegation norms. Important aspects such as the procedure for verifying identity documents or the technical and organisational requirements for the recognition of identity providers and security levels are to be regulated at the ordinance level.

In principle, this is appropriate in view of the dynamic environment and the high technical complexity in many areas. However, the Federal Council has a great responsibility to take into account the various concerns of all involved parties when implementing the ordinance. In this context, the Federal Council has also announced that it will open a consultation procedure for the ordinance.

Alongside the D-eID Act as the primary source of legislation governing digital identity in Switzerland, data protection regulations also play a pivotal role in the digital identity ecosystem, as elaborated in the previous section.

As the need to identify individuals is, in itself, nothing new, a number of other regulations have stipulated corresponding rules. While these regulations might not directly affect digital identity, it is essential to design and implement a digital identity solution in a way that is compatible with other relevant regulations to ensure its universal adoption.

For financial services companies in particular, the identification of new customers is already strictly regulated by Anti-Money-Laundering (AML) and Know-Your-Customer (KYC) regulations. Leveraging this experience and the supporting infrastructure and processes could provide a competitive edge for banks and insurance companies and enable them to take advantage of first-mover benefits in the market.



Electronic trust services

- Draft Federal Act on Electronic Identification Services (D-eID Act)
- Federal Act on Certified Electronic Signatures(CeS)
- Electronic identification and trust services for electronic transactions in the internal market (eIDAS)

Surveillance of post and telecommunications

- Federal Act on the Surveillance of Post and Telecommunications (SPTA)

Electronic patient record

- Federal Act on the Electronic Patient Record (EPR)

Data protection

- General Data Protection Regulation (GDPR)
- Federal Act on Data Protection (FADP) and Draft Federal Act on Data Protection (D-FADP)

KYC and AML

- Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB)
- Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA)

The Electronic Patient Record (EPR) is another high-profile digitalisation initiative in Switzerland that requires the secure and reliable identification of individuals to provide them with personal access to their treatment-related documents. It is envisioned that the eID will be linked with the Electronic Patient Record in the future.

In the area of electronic trust services, the Federal Act on Certified Electronic Signatures (CeS) defines different assurance levels with corresponding requirements for identification and authentication. With a view to international harmonisation, the CeS is conceived in a similar way to its European counterpart, the European Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

A comparison of the identity attributes required by each of these regulations reveals a heterogeneous picture with differing sets of identity attributes. Nevertheless, it is expected that the eID according to the Draft Federal Act on Electronic Identification Services (D-eID Act) can be used in these contexts, as the other regulations do not require additional identity attributes.

Besides the identity attributes themselves, it is important to consider and compare other relevant aspects of a digital identity ecosystem, such as the required metadata (e.g. which kind of identity document), the requirements for the verification process (e.g. physical presence vs. equivalent digital presence) and the different levels of security.

Identity attributes	Draft Federal Act on Electronic Identification Services (D-eID Act)	Federal Act on Certified Electronic Signatures (CeS)	Federal Act on the Electronic Patient Record (EPR)	CDB / Anti-Money Laundering Act	Federal Act on the Surveillance of Post and Telecommunications (SPTA)
Registration number	☑ Art. 5, para. 1, lit. a D-eID Act		☑ Art. 6, para. 2, lit. e EPR		
First name (official)	☑ Art. 5, para. 1, lit. c D-eID Act	☑ Art. 7, para. 2, lit. c CeS	☑ Art. 6, para. 2, lit. b EPR	☑ Art. 7 CDB 20	☑ Art. 20, para. 2, lit. a SPTA
Last name (official)	☑ Art. 5, para. 1, lit. b D-eID Act	☑ Art. 7, para. 2, lit. c CeS	☑ Art. 6, para. 2, lit. a EPR	☑ Art. 7 CDB 20	
Date of birth	☑ Art. 5, para. 1, lit. d D-eID Act		☑ Art. 6, para. 2, lit. d EPR	☑ Art. 7 CDB 20	☑ Art. 20, para. 2, lit. b SPTA
Place of birth	☑ Art. 5, para. 2, lit. b D-eID Act				
Gender	☑ Art. 5, para. 2, lit. a D-eID Act		☑ Art. 6, para. 2, lit. c EPR		
Nationality	☑ Art. 5, para. 2, lit. d D-eID Act			☑ Art. 7 CDB 20	
Facial image	☑ Art. 5, para. 3 D-eID Act				☑ Art. 20, para. 2, lit. f SPTA

□ Attribute not required ▨ Attribute required

6 Conclusion and outlook

Digital identity has the potential to become a catalyst for the end-to-end digital transformation of a wide range of business and government processes and thereby to increase efficiency, facilitate new products and create enhanced digital client interactions. In its absence, cumbersome and costly in-person identification is necessary in many cases, with existing digital identities inconveniently scattered across a multitude of different platforms.

In Switzerland, both the government and the market have recognised the need for a digital identity. With the Draft Federal Act on Electronic Identification Services (D-eID Act), the Swiss government has created a supporting regulatory framework to provide legal certainty for the private sector and protect the interests of individuals. In parallel to the legislative process, different private sector actors ranging from start-ups to a consortium of major Swiss companies have already seized the initiative and are actively developing and improving digital identity solutions – on different scales, with varying capabilities and supported by different underlying technology stacks.

From a technology perspective, emerging technologies have the potential to take centre stage in superseding today's scattered and outdated legacy identity systems. While biometrics could be used for capturing identity attributes and for authentication, blockchain technology has the potential to perform essential functions in the overall identity system and thereby mitigate the challenges associated with centralised systems.

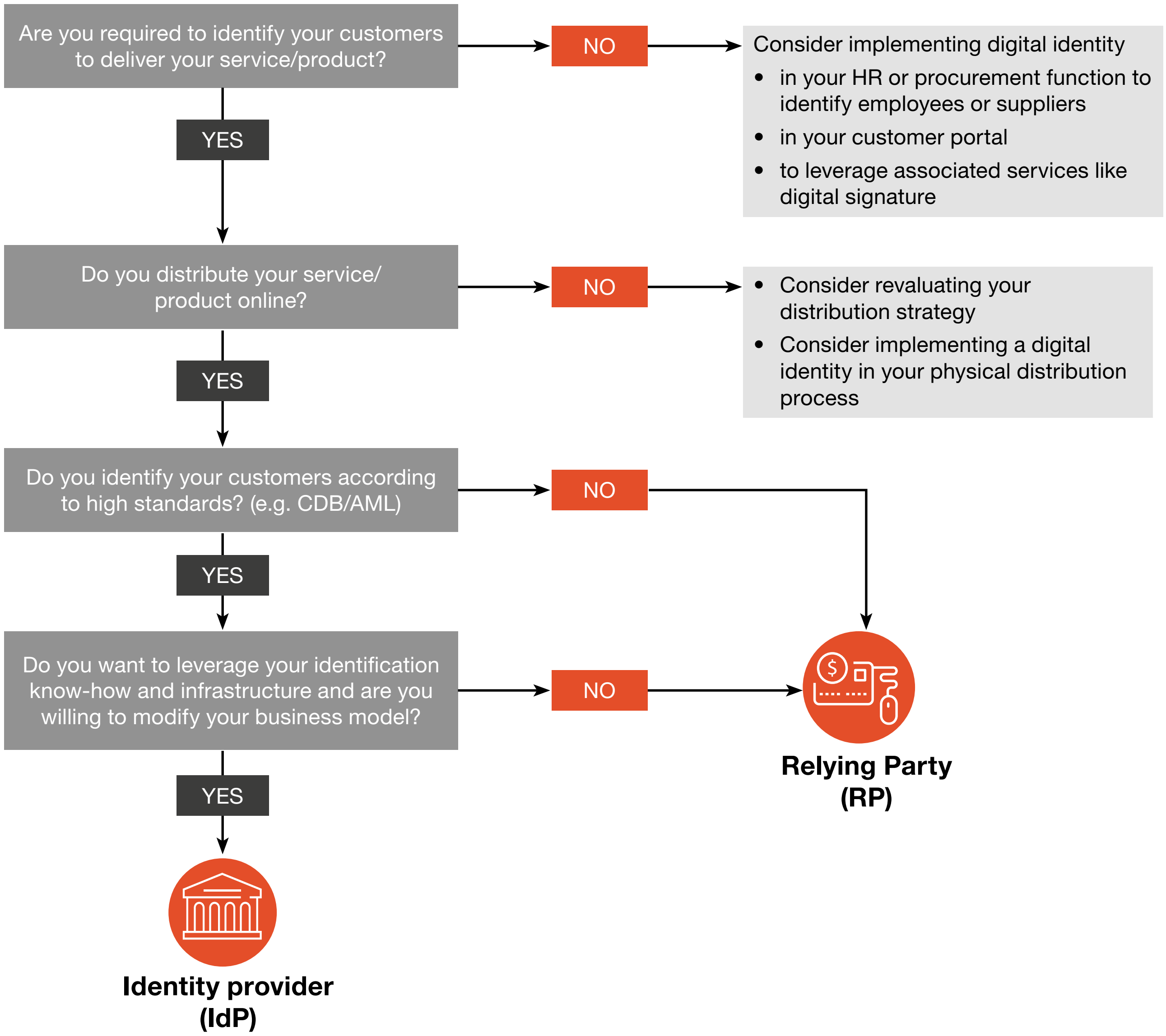
However, in a winner-takes-all market, only the best solution will gain users' trust and thereby reach the critical mass the Identity Provider needs in order to realise economies of scale and hence operate a sustainable business model. Building on the experience with TWINT, the Swiss ID consortium has to create a suitable incentive structure that allows competitors with potentially diverging interests to collaborate effectively and form a user-centric, digital identity ecosystem. If no suitable Swiss solution is developed soon, big tech companies like Google, Apple, Facebook or Amazon could quickly capitalise on the opportunity and create their own digital identity solution for Switzerland.

Independent of the ultimate Identity Provider, the real potential of digital identity comes into play when digital identity is leveraged for other fields. The possibilities are countless. Combined with the digital signature or the electronic patient record (EPR), digital identity can multiply the efficiency and convenience gains by facilitating seamlessly integrated digital products and services.

7 Call for action

7.1 Decision-tree – What is your company’s role in the digital identity ecosystem?

Embarking on the digital identity journey can yield significant benefits for both businesses and their customers. However, it can be challenging to identify the role your company should assume in the multifaceted digital identity ecosystem. By assessing your customer segment, distribution channel, identification standards and change capabilities, the decision tree depicted below can help you answer this question.



Are you required to identify your customers to deliver your service/product?

NO

Consider implementing digital identity

- in your HR or procurement function to identify employees or suppliers
- in your customer portal
- to leverage associated services like digital signature

YES

Do you distribute your service/product online?

NO

- Consider revaluating your distribution strategy
- Consider implementing a digital identity in your physical distribution process

YES

Do you identify your customers according to high standards? (e.g. CDB/AML)

NO

YES

Do you want to leverage your identification know-how and infrastructure and are you willing to modify your business model?

NO

Relying Party (RP)

YES

Identity provider (IdP)

7.2 How can PwC help you?

As a multi-disciplinary practice, we are uniquely positioned to help our clients adjust to the new environment. Our digital identity team includes strategists, consultants, lawyers, digital experts, cybersecurity specialists and technologists. Our global team of experienced business, technology and regulatory leaders can help you identify how digital identity can benefit your organisation and what you need to do to move your initiatives forward and achieve success.

Thanks to our extensive expertise in client onboarding, digitalisation and regulatory matters, we can help you design and implement the best solution for your business, from strategy to execution. Starting with an assessment of your current situation, we determine how your organisation can leverage digital identity to increase efficiency, enhance customer experience, and design and deliver a solution that is tailored to your businesses needs and in line with the relevant regulatory provisions.

1

Assessing the impact of digital identity on your business

Market and company assessment: Understand your role in the in the digital identity ecosystem and how digital identity impacts your overall strategy (e.g. market positioning, product portfolio and roadmap as well as distribution model).

2

Designing your digital identity operating model

2.1 Mandate for digital identity: Establish a board level mandate with clear purpose through a common strategy and secure sufficient funding.

2.2 Integrated digital identity solution: Identify your priorities and align the operating model with your firm's strategy and commercial objectives across the four foundational layers:

- **Strategy:** Go-to-market approach, product portfolio and distribuiton model
- **Experience:** User journey and flow across all channels (mobile, online, PoS)
- **Process:** On-boarding (incl. compliance checks), authentication and authorisation
- **Technology:** Front end (GUIs, CRM), back end (logic, data) and interfaces
- **Compliance:** Regulations, governance and contractual framework

3

Delivering your digital identity program

Implementation: Deploy your change the business capabilities to ensure transformation excellence through proven program management methodologies to deliver your digital identity solution at speed.

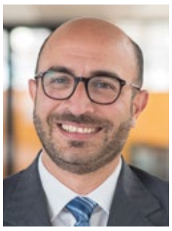
4

Handing over to business as usual

Continuous performance: Complete the transition of your digital identity program to your Business as Usual organisation and ensure your staff is fully trained and capable to run the delivered operating model.

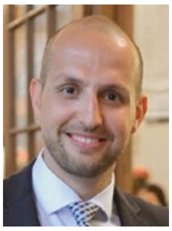
For more information please contact our experts

Advisory



Patrick Akiki
Partner, Management Consulting FS Lead
+41 79 708 11 07
akiki.patrick@ch.pwc.com

Holger Greif
Partner, Head Digital Banking Operations and Innovation
+41 58 792 13 86
holger.greif@ch.pwc.com



Morris Naqib
Director, Business Transformation and Regulatory Change
+41 79 902 31 45
morris.naqib@ch.pwc.com

Marc Lehmann
Director, Regulatory Transformation
+41 79 785 69 93
marc.lehmann@ch.pwc.com

Emanuel Staubli
Consultant, Management Consulting Financial Services
+41 79 709 10 49
emanuel.staubli@ch.pwc.com

Legal

Michael Taschner
Director, Head Strategic Legal Regulatory
+41 58 792 10 87
michael.taschner@ch.pwc.com

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00