

**strategy&**

*Part of the PwC network*

---

# Digital identity: Opportunities and challenges

**A perspective for  
telecom operators,  
banks, industrial  
companies and  
government  
institutions**



# Contacts

## France

Samer Kallas  
Partner,  
PwC Strategy& France  
+33-6- 8476-8898  
sam.kallas  
@strategyand.fr.pwc.com

## Turkey

Kağan Karamanoğlu  
Partner,  
PwC Strategy& Turkey  
+90-212-326-6309  
kagan.karamanoglu  
@strategyand.tr.pwc.com

## Dubai

Mohamed-Ali Benyoucef  
Manager,  
PwC Strategy& Dubai  
+971-56-156-7084  
mohamed.benyoucef  
@strategyand.ae.pwc.com

## About the authors

**Kağan Karamanoğlu** is a leading practitioner in the telecommunications and financial services industry for Strategy&, PwC's strategy consulting group. Based in Istanbul, he leads the Strategy& team in Turkey and is a member of the European Strategy& leadership team. With over 20 years of consulting and industry experience, Ka an specializes in corporate and business strategy and has led multiple client engagements globally.

**Samar Kallas** is a leading practitioner in telecommunications and technology sectors within Strategy&, PwC's strategy consulting group. He specializes in growth strategy, commercial due diligence, transformation programs and operating model design in addition to the representation of the Capabilities Driven Strategy and Fit for Growth offerings for PwC France. He has 12 years of experience in strategy consulting mainly in the telecom and Technology sectors.

**Mohamed-Ali Benyoucef** is a leading practitioner in telecommunications and technology sectors within Strategy&, PwC's strategy consulting group. Based in Dubai, he specializes in growth strategy and commercial due diligence, mainly in the Telecom and Technology sectors. He has more than 10 years of experience in strategy mainly in Telecoms and Technology sectors.

# 1. Digital ID: Inevitable growth

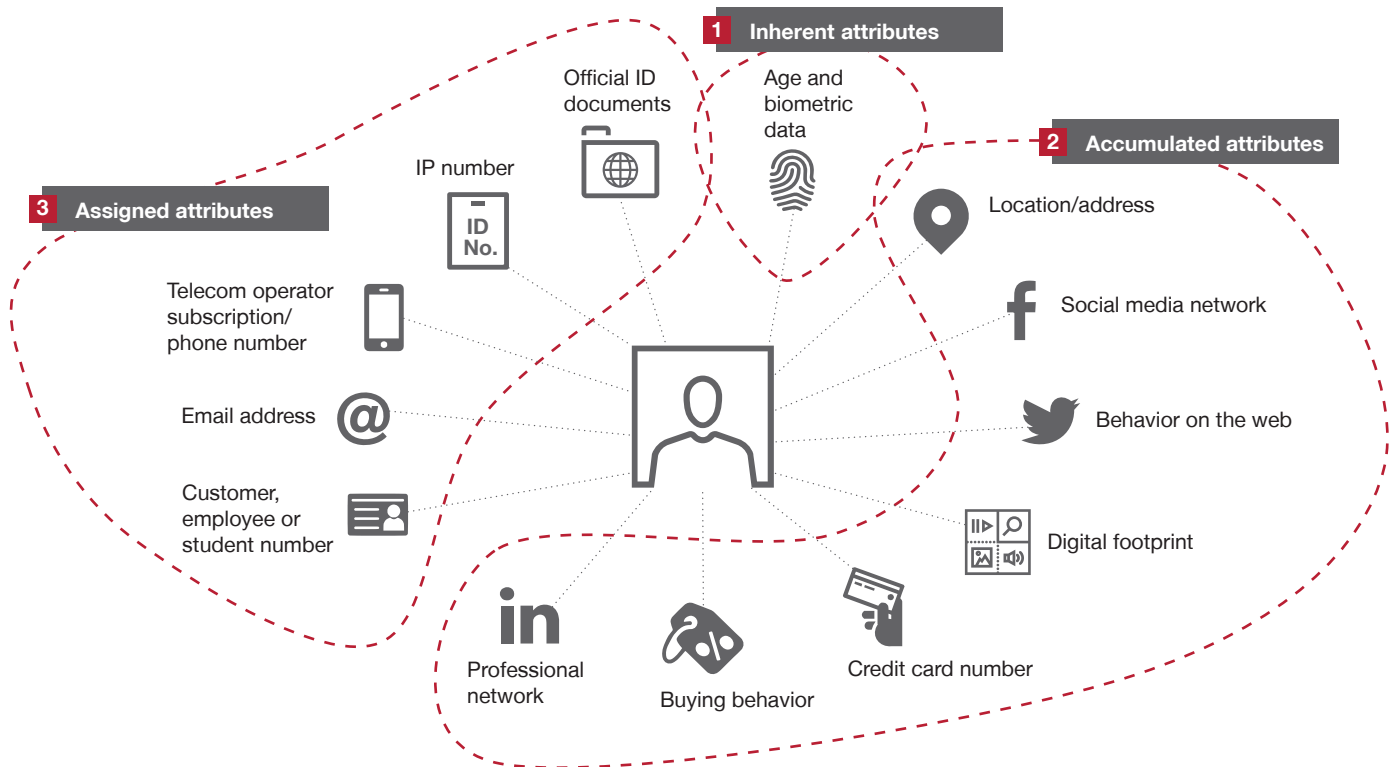
Digital disruption and technological advances are affecting the way people interact with companies and organizations. Many services, from accessing government benefits to signing into banking, are now being conducted digitally.

Given these developments, the growth of the digital identity market is inevitable. Digital identity (or digital ID) will continue to be adapted to serve as the identifier for accessing government services and benefits, as well as many other online services related to banking, the workplace, education and health. It is needed for creating accounts, making transactions and subscribing to services. It thus performs a vital function, enabling people to do their everyday work and save time, while at the same time maintaining their security. This paper seeks to highlight opportunities in the digital ID space by examining existing use cases, trends and best practices throughout the world. An individual's identity is a combination of inherent, accumulated, and assigned attributes (see *Exhibit 1*).

Currently, there are three digital ID systems being actively used in the market: centralized, third-party based and self-sovereign ID systems.

The first digital ID systems appeared in the 1990s, and were based on traditional state-owned centralized ID systems.

**EXHIBIT 1**  
Overview of the attributes that make up an individual's identity



Source: Strategy& analysis

In the early 2000s, with the proliferation of mobile telecommunications, digital banking and the emergence of social media platforms, users started to choose third parties they trusted to manage their digital identities. Private companies, acting as digital identity providers, and in some cases a federated ID system emerged. The government also continued to play a fundamental role at this stage, formulating and managing the identity framework and supporting these providers.

In the late 2010s, with more attention being paid to customer experience, data control and privacy, the self-sovereign ID system emerged. In this system, users are expected to take over the ownership and management of their identity traits (see *Exhibit 2*).

All three systems still exist today, and are widely used. However, these systems are still evolving due to changing socio-cultural norms and regulatory frameworks. For example, some e-government systems allow users to manage and control certain data. In these cases, individuals select which data (such as past health records) they are happy to share with a public entity.

Each system has both benefits and limitations. While centralized models introduce greater security and trust, decentralized models allow more user control and lead to an enhanced customer experience. In terms of limitations, the centralized model is exposed to the risk of system failure, while the decentralized model involves complex governance and carries a higher risk of identity theft.

**EXHIBIT 2**  
Available Digital ID Systems

	Centralized ID system	Federated ID system	Self-sovereign ID system
<b>Year of appearance</b>	1995	2006	2019
<b>Description</b>	A single provider – generally public – establishes and manages the identity of users	A trusted third party guarantees the user's identity to a service provider by transmitting or checking the user's attributes to the service provider	The user manages his/her identity based on a portfolio of attributes provided and verified by an ecosystem of attribute providers, and controls Telco players' access to his attributes
<b>Benefits</b>	Provides security and trust, especially in the KYC process	Users can have access to a wide range of services with a more efficient and seamless experience	Increased user control and trust resulting in a better user experience
<b>Dis-advantages</b>	Risk of system failure Required investment capacity Monopoly risk	Complexity (technical, governance)	Complex governance Technology under development Network effects take longer to initiate
<b>Examples</b>	e-Devlet Aadhaar Fedict Republic of Estonia Government	Facebook BankID itsme® Mobile Connect GOV.UK Turkcell ZenKey	ICONLOOP Turkcell Korea Financial Telecommunications and Clearings Institute

Source: World Bank, Telegeography, Strategy& analysis

---

### 1.1. Market size, key drivers and trends

The global digital ID market is predicted to be worth approximately US\$ 33 billion in 2025. This represents an increase from around US\$ 16 billion in 2020, with a CAGR of 16% over the five-year period (see *Exhibit 3*). The double-digit growth will principally result from a greater focus on customer experience, the escalating risk of cyber fraud and identity theft, and the increasing use of biometrics.

COVID-19 has accelerated the shift to digital processes including e-commerce. As a result, the e-commerce market was one of the fastest-growing verticals in 2020. In a bid to improve customer experience and help e-commerce players avoid organized fraud and cyberattacks, the use of digital ID solutions has proliferated in monetary transactions on e-commerce applications and platforms. Moreover, the increasing prevalence and use of electronic devices create a significant opportunity for market growth.

The swift adoption of e-government platforms shows the potential of the digital ID market, and creates an ideal foundation for considerable expansion. For example, in Turkey, the launch of the e-government gateway and the introduction of electronic ID led to the wider adoption of digital ID solutions, and hence stimulated market growth; with the e-government gateway reaching over 50 million users. Another strong indicator for growth is the electronic signature. There were close to 5 million e-signatures at the end of the first half of 2020 in Turkey, of which 700,000 were mobile signatures.

Logging into a bank's mobile app via e-government services is also a typical use case in financial services. In many countries, such as Germany, Spain, France and more recently, Turkey, it is possible to use banking services (such as opening an account) remotely by means of a digital ID authentication process (e-KYC).

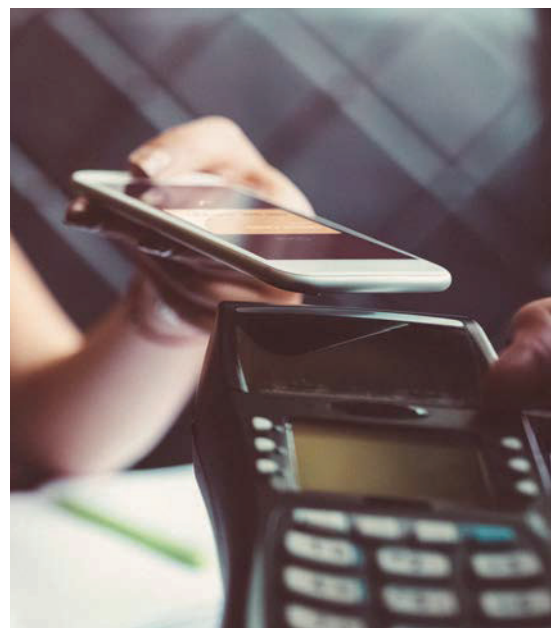
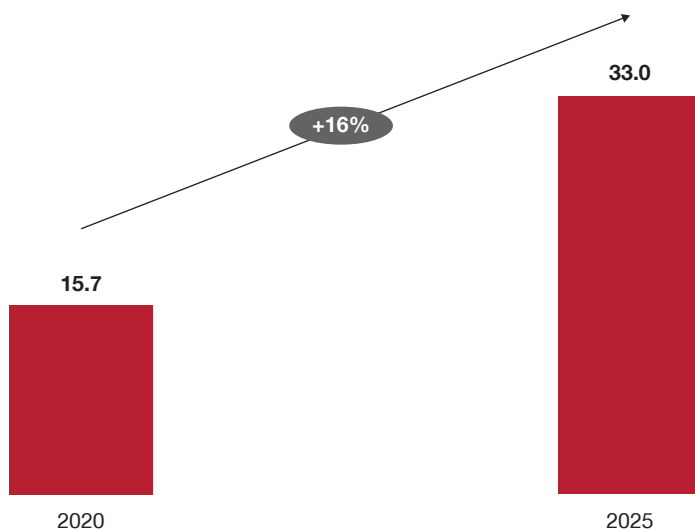
---

#### EXHIBIT 3

#### Global digital ID market overview

---

#### Global digital identity solutions market size (USD bn)



Source: Globalnewswire, Markets and Markets, IDC, Strategy& analysis

---

## 1.2. Market segments

There are two main segments for digital ID applications: business-to-business (B2B) and business-(to-business)-to-consumer (B2(B2)C).



The B2B model primarily enables corporate and government organizations to identify their employees. This model incorporates services such as identity management in enterprises, and employee access to enterprise services.



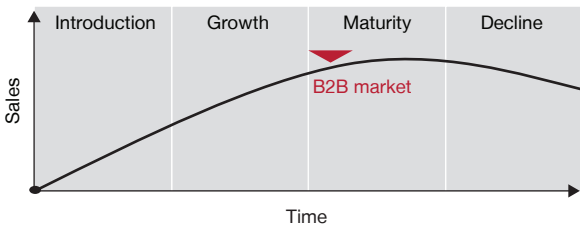
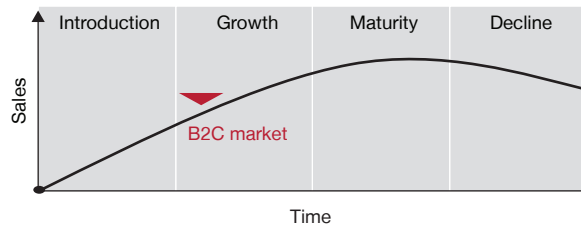


The B2(B2)C model enables service providers to identify their customers. This includes services such as creating accounts, managing subscriptions and authenticating transactions.

The B2B market is highly mature. Solutions are now well established, and the relevant players have regular revenue models (for example, through offering software-as-a-service (SaaS), or licenses). On the other hand, B2(B2)C could be classified as an emerging market, as it possesses only embryonic revenue models and faces certain challenges (see *Exhibit 4*).

### EXHIBIT 4

#### Key characteristics of the B2B and B2(B2)C market

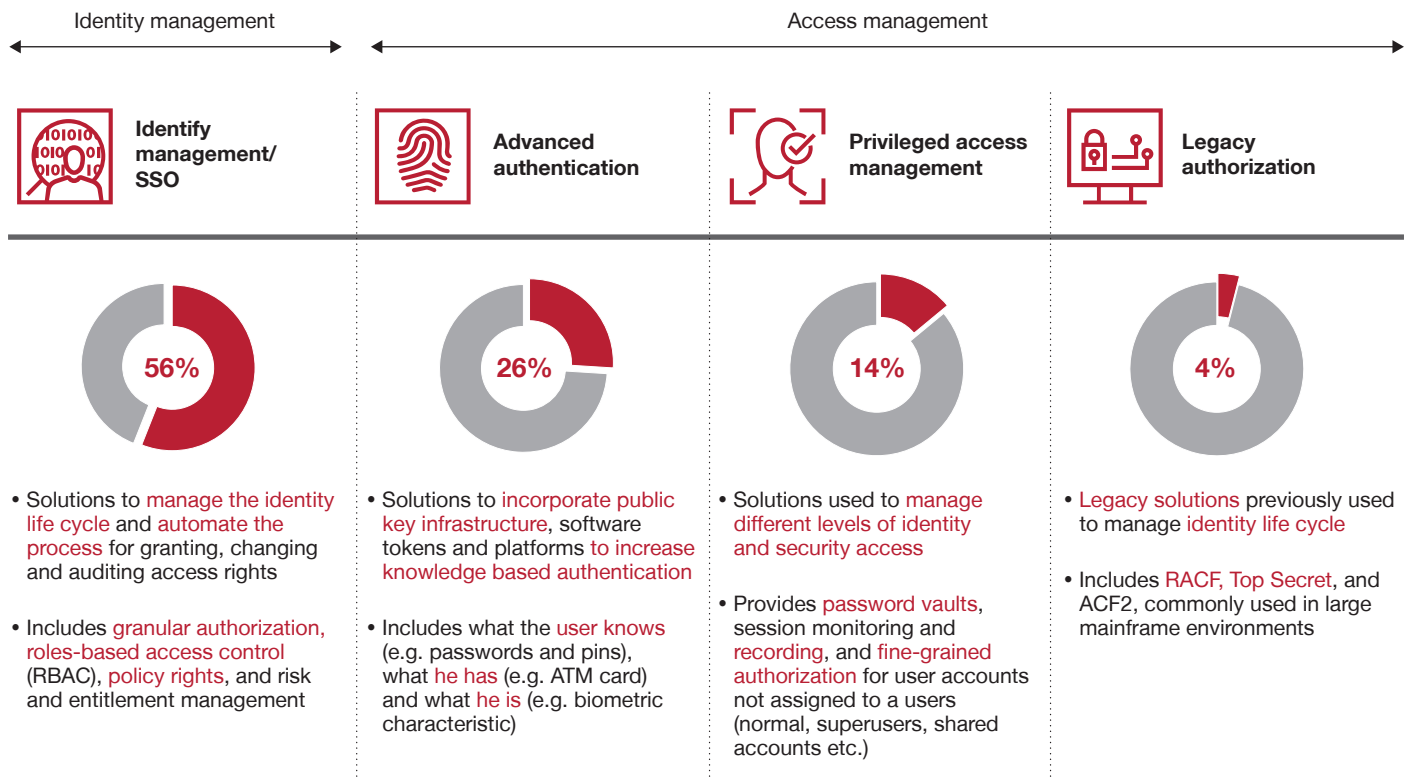
	 <b>B2B market</b>	 <b>B2C/B2B2C market</b>
<b>Clients</b>	<ul style="list-style-type: none"> <li>Public or private organizations (e.g. companies, governments)</li> </ul>	<ul style="list-style-type: none"> <li>End-users (e.g. internet surfers, application users)</li> <li>Service providers</li> </ul>
<b>Revenue model</b>	<ul style="list-style-type: none"> <li>Paid</li> <li>Software revenue models (e.g. subscription, license etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Mostly free for end users</li> <li>Revenues from service providers</li> </ul>
<b>Value proposition</b>	<ul style="list-style-type: none"> <li>Provide organizations with solutions to manage the access, authentication and the identification of their employees or clients (e.g. identity management)</li> </ul>	<ul style="list-style-type: none"> <li>Provide a verified identity and/or secure transactions for Telco players (e.g. database check, document verification, authentication, etc.)</li> </ul>
<b>Market maturity</b>		

Source: Strategy& analysis

The B2B market comprises two segments, namely identity management and access management. Most of the market is concentrated on identity management/single sign-on (SSO) and advanced authentication, which is an element of access management (see Exhibit 5).

**EXHIBIT 5**

B2B identity market segments: in 2020, % of worldwide market spend in m\$



Source: IDC, Strategy& analysis



The B2B identity market is concentrated on identity management/single sign-on (SSO) and advanced authentication, which includes what the user knows, s/he has and s/he is.”

B2(B2)C is built around access management, consisting of both identification and authentication. New account creation and subscription to applications or platforms are the identification use cases for identification, while logging-in services and transaction authentication are the main use cases for the latter (see *Exhibit 6*).

**EXHIBIT 6**  
B2(B2)C Digital ID market segments

	A Identification (ID verification)		B User authentication		
	Checking against a database	Official document/ biometric check	SFA	MFA	RBA
<b>Description</b>	Cross-check the identity of the new user with that of one or more service provider databases	Prove that the specific attributes are related to the user	Authenticate the registered user with a single factor	Authenticate the registered user through multiple factors of his/her choosing	Authenticate the registered user through multiple factors, related to fraud control
<b>Examples</b>	Match the user's ID with: the identity of his operator, a bank account, or a credit bureau, etc.	Users scan or read their ID cards and take a video of their face	A login/password pair	The association of: a login/password pair, a terminal, a SIM card, a PKI key, etc.	Fraud alerts: MSISDN, contract holder, certificate of residence, SIM swap, call forward, purchasing behavior, location, etc.
<b>Selected benchmarks</b>	<div style="border: 1px solid gray; padding: 5px; text-align: center;">AXA</div> Subscription to an insurance contract	<div style="border: 1px solid gray; padding: 5px; text-align: center;">Airbnb</div> Creating new accounts	<div style="border: 1px solid gray; padding: 5px; text-align: center;">Facebook</div> Login to the service	<div style="border: 1px solid gray; padding: 5px; text-align: center;">3-D Secure</div> Transaction authentication	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid gray; padding: 5px; text-align: center;">Amazon</div> <div style="border: 1px solid gray; padding: 5px; text-align: center;">Fnac</div> </div> Reducing fraud in online transactions

Source: Strategy& analysis

“B2(B2)C digital ID market is built around identification such as checking against a database and authentication including single and multiple factor authentication.”

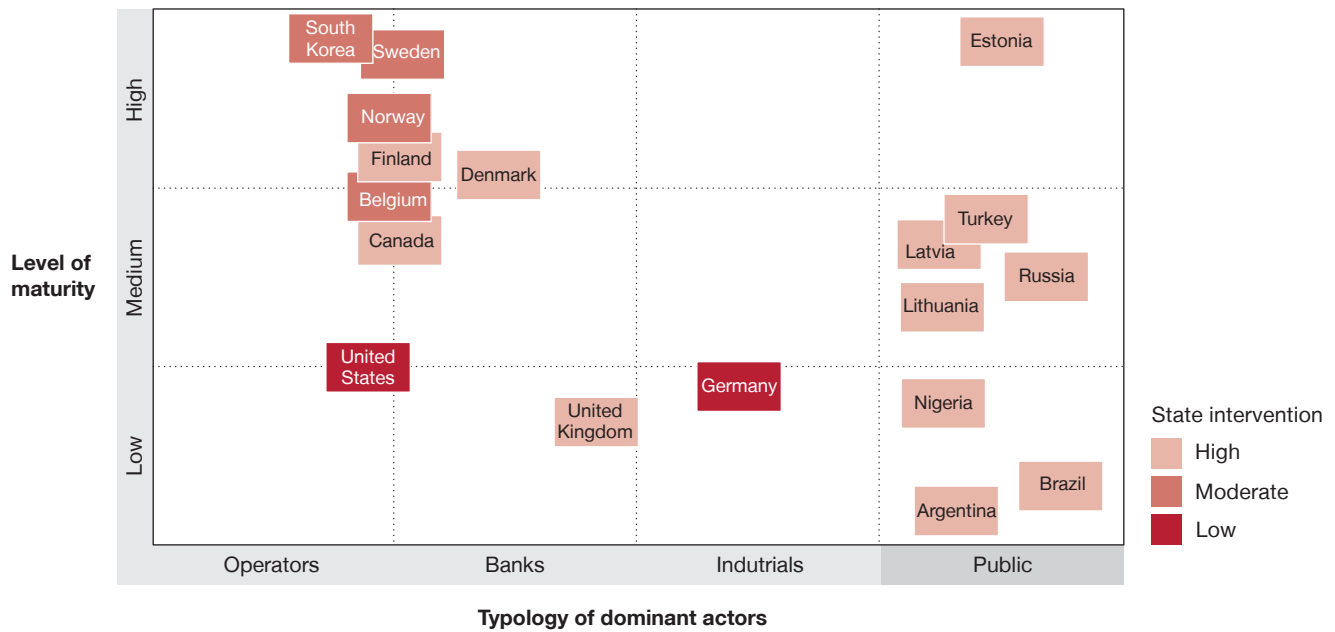


### 1.3. Key success factors

Telecom operators, banks, industrials and public institutions have all contributed to the development of digital ID solutions in various countries. Different levels of maturity are evident in each country (see Exhibit 7).

#### EXHIBIT 7

Overview of different Digital identity models



Source: Strategy& analysis











There are various key success factors that are common to successful markets:

1. A trustworthy and transparent solution is essential for giving new users an adequate level of confidence.
2. A favorable regulatory environment stimulates digital ID usage in a given country.
3. Solutions should have the maximum possible exposure. Digital ID providers can collaborate and/or create a consortium with several other players from various industries to ensure that this happens (this has occurred, for example, in the United States and Germany).
4. The design of the user experience is critical, with a seamless integration between service and digital ID solution providers.
5. Finally, the business models should be very simple and offer free solutions to end users (see *Exhibit 8*).

**EXHIBIT 8**

Overview of success criteria for the rapid development of a viable and sustainable Digital Identity solution

	A Service providers	B End users
Relevance and transparency of the solution	 <p>Robust identity attribute verification with a <b>high level of security</b>, used for the Identity Providers's <b>own customers</b></p>	 <p><b>User confidence</b>: commitment in terms of data protection, technologies, etc.</p>
Suitable for network effects	 <p><b>Broad coverage of the population</b> with a single solution combined with the possibility of covering the entire population</p>	 <p>Adoption of the solution by <b>service provider partners</b></p>
Simple to use, generating little interference	 <p><b>Seamless integration between Service Provider and Identity Solution Provider UX</b>: neutral branding, simplified path, etc.</p>	 <p><b>Ease of use of the solution</b> for the end user</p>
Simplicity of the business model	 <p><b>Simplicity of the pricing model</b>, based on a <b>volumetric model</b>: free-for-service or per user</p>	 <p><b>Free solution for the end user</b></p>

Source: Strategy& analysis

---

#### 1.4. Issues, risks and threats

As they face many challenges and risks, very few markets and players have managed to achieve secure and transparent identification and authentication processes at scale. Today, the key issues for digital ID providers are:

---

##### 1. Regulation



The authorities must put in place clear and stable rules on how personal data should be collected, processed and shared. In addition, regulations that encourage the usage of digital ID, for example in South Korea with an obligation to check the age of user for all e-commerce transactions, boosted the adoption of this technology and created a well-developed ecosystem beyond this particular use-case.

---

##### 2. Customer experience



As digitalization has placed customers at the center of a company's business operations and offerings, they need to be provided with a seamless experience. Indeed, this has become a prerequisite for all digital applications. Players need to pay attention to the customer journey and focus on launching customer-centric solutions. Finding the right balance between security and convenience is one of the most significant challenge for digital ID solution providers.

---

##### 3. Scale and coverage



One of the main obstacles involves persuading users to adopt digital ID solutions. In order to achieve an efficient and trustworthy system, digital ID providers need to have a broad customer base spanning various customer segments. However, users tend to avoid unproven systems, which in turn prevents further development of the services (the chicken and egg syndrome).

---

##### 4. Monetization



Players should monetize those solutions for which end users are reluctant to pay additional fees for digital ID applications. There is a growing number of use cases for which users are willing to pay, particularly in developed European countries, yet the volume of such cases is still limited.

---













## 2. Collaboration and scale are essential

From our analysis and discussions with industry leaders, we have seen that digital IDs are used for numerous applications. Telecom operators, banks, industrials and governments are actively seeking opportunities so that they can maintain their differentiation in the marketplace. In many markets, these players often collaborate to launch or participate in digital identity solutions. These collaborative ventures are more likely to be successful (see *Exhibit 9*).

For example, Verified.Me is a digital ID platform in Canada, offered by SecureKey Technologies Inc., and developed in cooperation with seven major financial institutions of Canada – BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD. Verified.Me helps citizens to verify their identity quickly and securely by consenting to the use of selected personal information, thus reducing oversharing of information. The profile can be linked with various services such as a credit bureau, insurance providers or health centers.

Forming a consortium is critical to generating the necessary scale when players in the same industry, or from different industries, seek to offer digital ID solutions. Zenkey in the United States is an example of such a consortium. It was established by a joint venture of American mobile network operators, offering an improved and streamlined customer experience, combined with greater control over private data, thus differentiating itself from competitors. It is positioned as a straightforward interface between digital ID providers and mobile operators. Zenkey uses the joint database of the operators, hence the required attributes for creating an account have been simplified somewhat. It uses face ID and enables users to fill out forms, and make quick and secure registrations, while ensuring identity authentication.

**EXHIBIT 9**  
Examples of initiatives initiated by or with operators and main lessons learned

One operator	Collaboration with ...									
	... all operators					... banks			... of industrialists	
										
Turkcell	PASS	ZenKey	Mobile connect	MobileID	Mobiil-ID	BankID	itsme®	Verified.Me	Verimi	
50% market share, 2 <sup>nd</sup> application dev. Coverage by OTT from 2017	Interoperability of solutions from 2015 onwards after 10 years of independence	Creation of a JV between all operators in 2018 Launch in 2019	Gathering around Mobile Connect in 2017 thanks to a technology hub (WSO2.Telco)	Gathering around Mobile Connect in 2017	Creation of a JV in 2007 Opening to other operators from 2009	Creation of a JV in 2009 then opening to other operators	Creation of a JV in 2016 Launch of Itsme in 2017	Creation of a JV between operators in 2018 to participate in SecureKey	Creation of a JV in 2017 Launch in 2018	
 1	3	4	7	4	3	3	1	4	1	
 X	Consortium	✓	Common technological hub	✓	✓	✓	✓	✓	✓	✓

Source: Strategy& analysis

---

Some initiatives are trying to achieve scale nationally by onboarding as much businesses as possible such as connectID in Australia, which combines digital ID with payments and loyalty programs. As a mass-market digital identity hub for the Australian digital ecosystem, connectID is backed by top banks and retailers. The system is developed by the electronic payment scheme EFTPOS, which has access to more than 40 million bank accounts. By seamlessly connecting all identity requests from financial services, telecom operators, online stores and government departments with digital ID issuers in Australia, connectID enables companies to streamline their customer experience in a secure, private, simple and trusted way.

The experience of these players offers some important lessons that telecom operators, banks, industrials and governments should be aware of:

- Success requires security and superior user experience.
- To extend capabilities, achieve scale and expand the customer base for the digital ID solution, collaboration between players from the same and different verticals is very common.
- Bundling identity solutions with value-added services can increase adoption.
- Governments need to create a well-constructed regulatory background to promote adoption of digital ID propositions. This is essential for the market to work effectively.
- Digital ID solutions can improve risk management for banks and facilitate know-your-customer (KYC) processes, as well as improving customer experience and boosting productivity.
- Digital ID providers can attract service providers through revenue sharing and early adopter discounts.
- In the long term, B2C monetization via a subscription model might offer a significant opportunity.
- Telecom operators are more likely to adopt cross-carrier solutions rather than act alone.

On the other hand, some other initiatives have to date struggled to deliver successful digital identity solutions. There are also key lessons to be learned from these unsuccessful cases:

- To increase customer engagement, digital ID services should be free of charge for end users.
- The onboarding process needs to be seamless.
- Governments should encourage collaboration with relevant verticals.
- Solutions are more successful if they are combined with value-added services.
- An adequate number of use cases is critical for increasing adoption and consumer trust.

---

### 3. Conclusion: How to succeed

Digital ID providers must take a step back and adopt a systematic approach. To succeed and expand in their field, they need to answer certain vital questions, and carefully assess the current market, learning from past successes and failures.

The key questions they need to ask themselves are:

What positioning across the value chain is optimal in order to maximize value creation? (for example, it is important to decide whether to be an attribute provider, a digital ID solution provider or a solution reseller)



What is the right promotion/marketing strategy and go-to-market strategy for each segment or vertical?



As well as direct value, what are the significant future opportunities for service providers? (such as financial identity and alternative credit scoring, KYC data offering, government partnership or regional expansion)



Are there any opportunities to embrace innovation in partnership or a consortium with other digital or technology companies?



What are the main pillars of a go-to-market plan? What are the key milestones? How should success be measured?



---

Through answering these questions, telecom operators, banks, industrials and government institutions can discover major opportunities and enhance their operations in the digital identity market.

**1**

Digital ID providers have the opportunity to succeed in a crowded market, as the issue of secure, seamless authentication has still not been resolved. Identity is a highly competitive area. In this context, a rapid go-to-market strategy is critical.

**2**

Players can pursue different value levers, such as identity verification services (IDV), attribute aggregation, user authentication and others, such as advertising or fraud analytics.

**3**

A successful go-to-market strategy involves considering market potential and the relevant players' right to win, and then prioritizing industry verticals and use cases. An initial strategic focus on selected verticals, such as e-commerce, media, healthcare, and financial services can lead to a significant advantage.

**4**

Intensifying competition, especially from biometric-based and document authentication technologies, may pose a threat to digital ID providers. The players should therefore consider adding biometrics and behavioral capabilities through partnerships or acquisitions.

**5**

It is possible to reduce costs through a streamlined KYC process, better fraud and risk management, and improved compliance with regulation. With the benefit of digital ID, service providers would ultimately become less prone to errors, achieve more operational efficiency, and build several cost-cutting synergies.

**6**

Digital ID enables service providers to expand their customer base by streamlining the onboarding processes and ensuring data security. Moreover, digital ID allows them to launch more complex products, thereby attracting more customers.

**7**

Governments must play a significant role in the proliferation of digital ID solutions. They need to encourage the private sector to cooperate, and support companies in launching and expanding digital ID solutions.

Digital ID providers should constantly adapt their strategic positioning within the value chain. By prioritizing customer segments with the highest potential and partnering with relevant solution providers, players can secure the right to win in this burgeoning market.

# strategy&

Part of the PwC network

---

## Strategy&

Strategy& is a global strategy consulting business uniquely positioned to help deliver your best future: one that is built on differentiation from the inside out and tailored exactly to you. As part of PwC, every day we're building the winning systems that are at the heart of growth. We combine our powerful foresight with this tangible know-how, technology, and scale to help you create a better, more transformative strategy from day one.

As the only at-scale strategy business that's part of a global professional services network, we embed our strategy capabilities with frontline teams across PwC to show you where you need to go, the choices you'll need to make to get there, and how to get it right.

The result is an authentic strategy process powerful enough to capture possibility, while pragmatic enough to ensure effective delivery. It's the strategy that gets an organization through the changes of today and drives results that redefine tomorrow. It's the strategy that turns vision into reality. It's strategy, made real.

[www.strategyand.pwc.com](http://www.strategyand.pwc.com)